LD8395

IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL
MONOGRAPHS

Volume 245

Fermat's Last Theorem

The Proof

Takeshi Saito

American Mathematical Society

Fermat's Last Theorem

The Proof

IWANAMI SERIES IN MODERN MATHEMATICS

Translations of
MATHEMATICAL
MONOGRAPHS

Volume 245

Fermat's Last Theorem

The Proof

Takeshi Saito

Translated from the Japanese by
Masato Kuwata

American Mathematical Society
Providence, Rhode Island

FERUMA YOSO (Fermat Conjecture)
フェルマー予想
by Takeshi Saito
斎藤　毅
© 2009 by Takeshi Saito
First published 2009 by Iwanami Shoten, Publishers, Tokyo.
This English language edition published in 2014
by the American Mathematical Society, Providence
by arrangement with the author c/o Iwanami Shoten, Publishers, Tokyo
Translated from the Japanese by Masato Kuwata

2010 *Mathematics Subject Classification.* Primary 11D41;
Secondary 11F11, 11F80, 11G05, 11G18.

Library of Congress Cataloging-in-Publication Data
ISBN 978-0-8218-9849-9 Fermat's last theorem: the proof
(Translations of mathematical monographs ; volume 245)
The first volume was catalogued as follows:
Saito, Takeshi, 1961–
Fermat's last theorem: basic tools / Takeshi Saito ; translated by Masato Kuwata.—English language edition.
pages cm.—(Translations of mathematical monographs ; volume 243)
First published by Iwanami Shoten, Publishers, Tokyo, 2009.
Includes bibliographical references and index.
ISBN 978-0-8218-9848-2 (alk. paper)
1. Fermat's last theorem. 2. Number theory. 3. Algebraic number theory. I. Title. II. Title: Fermat's last theorem: basic tools.

QA244.S2513 2013
512.7'4–dc23

2013023932

© 2014 by the American Mathematical Society. All rights reserved.
The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.

Information on copying and reprinting can be found in the back of this volume.

Visit the AMS home page at `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 19 18 17 16 15 14

Contents

Basic Tools

Preface xi

Preface to the English Edition xvii

Chapter 0. Synopsis 1
0.1. Simple paraphrase 1
0.2. Elliptic curves 3
0.3. Elliptic curves and modular forms 5
0.4. Conductor of an elliptic curve and level of a modular form 7
0.5. ℓ-torsion points of elliptic curves and modular forms 9

Chapter 1. Elliptic curves 13
1.1. Elliptic curves over a field 13
1.2. Reduction mod p 15
1.3. Morphisms and the Tate modules 22
1.4. Elliptic curves over an arbitrary scheme 26
1.5. Generalized elliptic curves 29

Chapter 2. Modular forms 35
2.1. The j-invariant 35
2.2. Moduli spaces 37
2.3. Modular curves and modular forms 40
2.4. Construction of modular curves 44
2.5. The genus formula 52
2.6. The Hecke operators 55
2.7. The q-expansions 58
2.8. Primary forms, primitive forms 62
2.9. Elliptic curves and modular forms 65

2.10. Primary forms, primitive forms, and Hecke algebras 66
2.11. The analytic expression 70
2.12. The q-expansion and analytic expression 74
2.13. The q-expansion and Hecke operators 77

Chapter 3. Galois representations 81
3.1. Frobenius substitutions 82
3.2. Galois representations and finite group schemes 86
3.3. The Tate module of an elliptic curve 89
3.4. Modular ℓ-adic representations 91
3.5. Ramification conditions 96
3.6. Finite flat group schemes 100
3.7. Ramification of the Tate module of an elliptic curve 103
3.8. Level of modular forms and ramification 108

Chapter 4. The 3–5 trick 111
4.1. Proof of Theorem 2.54 111
4.2. Summary of the Proof of Theorem 0.1 116

Chapter 5. $R = T$ 119
5.1. What is $R = T$? 119
5.2. Deformation rings 122
5.3. Hecke algebras 126
5.4. Some commutative algebra 131
5.5. Hecke modules 135
5.6. Outline of the Proof of Theorem 5.22 137

Chapter 6. Commutative algebra 143
6.1. Proof of Theorem 5.25 143
6.2. Proof of Theorem 5.27 149

Chapter 7. Deformation rings 159
7.1. Functors and their representations 159
7.2. The existence theorem 161
7.3. Proof of Theorem 5.8 162
7.4. Proof of Theorem 7.7 166

Appendix A. Supplements to scheme theory 171
A.1. Various properties of schemes 171
A.2. Group schemes 175
A.3. Quotient by a finite group 177
A.4. Flat covering 178

A.5. G-torsor 179
A.6. Closed condition 182
A.7. Cartier divisor 183
A.8. Smooth commutative group scheme 185

Bibliography 189

Symbol Index 197

Subject Index 199

The Proof

Preface ix

Preface to the English Edition xv

Chapter 8. Modular curves over **Z** 1
- 8.1. Elliptic curves in characteristic $p > 0$ 1
- 8.2. Cyclic group schemes 6
- 8.3. Drinfeld level structure 12
- 8.4. Modular curves over **Z** 20
- 8.5. Modular curve $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ 25
- 8.6. Igusa curves 32
- 8.7. Modular curve $Y_1(N)_{\mathbf{Z}}$ 37
- 8.8. Modular curve $Y_0(N)_{\mathbf{Z}}$ 41
- 8.9. Compactifications 48

Chapter 9. Modular forms and Galois representations 61
- 9.1. Hecke algebras with **Z** coefficients 61
- 9.2. Congruence relations 70
- 9.3. Modular mod ℓ representations and non-Eisenstein ideals 76
- 9.4. Level of modular forms and ramification of ℓ-adic representations 81
- 9.5. Old part 90
- 9.6. Néron model of the Jacobian $J_0(Mp)$ 97
- 9.7. Level of modular forms and ramification of mod ℓ representations 102

Chapter 10. Hecke modules 107
10.1. Full Hecke algebras 108
10.2. Hecke modules 113
10.3. Proof of Proposition 10.11 118
10.4. Deformation rings and group rings 125
10.5. Family of liftings 129
10.6. Proof of Proposition 10.37 136
10.7. Proof of Theorem 5.22 140

Chapter 11. Selmer groups 143
11.1. Cohomology of groups 143
11.2. Galois cohomology 149
11.3. Selmer groups 157
11.4. Selmer groups and deformation rings 161
11.5. Calculation of local conditions and proof of Proposition 11.38 165
11.6. Proof of Theorem 11.37 169

Appendix B. Curves over discrete valuation rings 179
B.1. Curves 179
B.2. Semistable curve over a discrete valuation ring 182
B.3. Dual chain complex of curves over a discrete valuation ring 187

Appendix C. Finite commutative group scheme over $\mathbf{Z}_p$ 191
C.1. Finite flat commutative group scheme over $\mathbf{F}_p$ 191
C.2. Finite flat commutative group scheme over $\mathbf{Z}_p$ 192

Appendix D. Jacobian of a curve and its Néron model 199
D.1. The divisor class group of a curve 199
D.2. The Jacobian of a curve 201
D.3. The Néron model of an abelian variety 205
D.4. The Néron model of the Jacobian of a curve 209

Bibliography 213

Symbol Index 217

Subject Index 221

Preface

It has been more than 350 years since Pierre de Fermat wrote in the margin of his copy of *Arithmetica* of Diophantus:

> It is impossible to separate a cube into two cubes, or a biquadrate into two biquadrates, or in general any power higher than the second into powers of like degree; I have discovered a truly remarkable proof which this margin is too small to contain.[1]

This is what we call Fermat's Last Theorem. It is certain that he has a proof in the case of cubes and biquadrates (i.e., fourth powers), but it is now widely believed that he did not have a proof in the higher degree cases. After enormous effort made by a great number of mathematicians, Fermat's Last Theorem was finally proved by Andrew Wiles and Richard Taylor in 1994.

The purpose of this book is to give a comprehensive account of the proof of Fermat's Last Theorem. Although Wiles's proof is based on very natural ideas, its framework is quite complex, some parts of it are very technical, and it employs many different notions in mathematics. In this book I included parts that explain the outline of what follows before introducing new notions or formulating the proof formally. Chapter 0 and §§5.1, 5.5, and 5.6 in Chapter 5 are those parts. Logically speaking, these are not necessary, but I included these in order to promote better understanding. Despite the aim of this book, I could not prove every single proposition and theorem. For the omitted proofs please consult the references indicated at the end of the book.

The content of this book is as follows. We first describe the rough outline of the proof. We relate Fermat's Last Theorem with elliptic curves, modular forms, and Galois representations. Using these relations, we reduce Fermat's Last Theorem to the modularity of certain ℓ-adic representations (Theorem 3.36) and a theorem on the level of mod ℓ representations (Theorem 3.55). Next, we introduce the notions of deformation rings and Hecke algebras, which are incarnations of Galois representations and modular forms, respectively. We then prove two theorems on commutative algebra. Using these theorems, we reduce Theorem 3.36 to certain properties of Selmer groups and Hecke modules, which are also incarnations of Galois representations and modular forms.

---

[1] Written originally in Latin. English translation is taken from Dickson, L. E., *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966.

We then construct fundamental objects, modular curves over $\mathbf{Z}$, and the Galois representations associated with modular forms. The latter lie in the foundation of the entire proof. We also show a part of the proof of Theorem 3.55. Finally, we define the Hecke modules and the Selmer groups, and we prove Theorem 3.36, which completes the proof of Fermat's Last Theorem.

The content of each chapter is summarized at its beginning, but we introduce them here briefly. In Chapter 0,* we show that Fermat's Last Theorem is derived from Theorem 0.13, which is about the connection between elliptic curves and modular forms, and Theorem 0.15, which is about the ramification and level of ℓ-torsion points of an elliptic curve. The objective of Chapters 1–4* is to understand the content of Chapter 0 more precisely. The precise formulations of Theorems 0.13 and 0.15 will be given in Chapters 1–3. In the proof presented in Chapter 0, the leading roles are played by elliptic curves, modular forms, and Galois representations, each of which will be the main theme of Chapters 1, 2, and 3. In Chapter 3, the modularity of ℓ-adic representations will be formulated in Theorem 3.36. In Chapter 4, using Theorem 4.4 on the rational points of an elliptic curve, we deduce Theorem 0.13 from Theorem 3.36. In §4.2, we review the outline of the proof of Theorem 0.1 again.

In Chapters 5–7,* we describe the proof of Theorem 3.36. The principal actors in this proof are deformation rings and Hecke algebras. The roles of these rings will be explained in §5.1. In Chapter 5, using two theorems of commutative algebra, we deduce Theorem 3.36 from Theorems 5.32, 5.34, and Proposition 5.33, which concern the properties of Selmer groups and Hecke modules. The two theorems

---

*Chapters 0–7 along with Appendix A appeared in *Fermat's Last Theorem: Basic Tools*, a translation of the Japanese original.

in commutative algebra will be proved in Chapter 6. In Chapter 7, we will prove the existence theorem of deformation rings.

In Chapter 8, we will define modular curves over **Z** and study their properties. Modular forms are defined in Chapter 2 using modular curves over **Q**, but their arithmetic properties are often derived from the behavior of modular curves over **Z** at each prime number. Modular curves are known to have good reduction at primes not dividing their levels, but it is particularly important to know their precise properties at the prime factors of the level. A major factor that made it possible to prove Fermat's Last Theorem within the twentieth century is that properties of modular curves over **Z** had been studied intensively. We hope the reader will appreciate this fact.

In Chapter 9, we construct Galois representations associated with modular forms, using the results of Chapter 8, and prove a part of Theorem 3.55 which describes the relation between ramification and the level. Unfortunately, however, we could not describe the celebrated proof of Theorem 3.55 in the case of $p \equiv 1 \bmod \ell$ by K. Ribet because it requires heavy preparations, such as the p-adic uniformization of Shimura curves and the Jacquet–Langlands–Shimizu correspondence of automorphic representations.

In Chapter 10, using results of Chapters 8 and 9, we construct Hecke modules as the completion of the singular homology groups of modular curves, and we then prove Theorem 5.32(2) and Proposition 5.33. In Chapter 11, we introduce the Galois cohomology groups and define the Selmer groups. Then we prove Theorems 5.32(1) and 5.34. The first half of Chapter 11 up to §11.3 may be read independently as an introduction to Galois cohomology and the Selmer groups.

Throughout the book, we assume general background in number theory, commutative algebra, and general theory of schemes. These are treated in other volumes in the Iwanami series: *Number Theory 1*, *2*, and *3*, *Commutative algebras and fields* (no English translation), and *Algebraic Geometry* 1 and 2. For scheme theory, we give a brief supplement in Appendix A after Chapter 7. Other prerequisites are summarized in Appendices B, C, and D at the end of the volume.

In Appendix B, we describe algebraic curves over a discrete valuation rings and semistable curves in particular, as an algebro-geometric preparation to the study of modular curves over **Z**. In Appendix C, we give a linear algebraic description of finite flat commutative group schemes over $\mathbf{Z}_p$, which will be important for the study of p-adic

Galois representations of p-adic fields. Finally, in Appendix D, we give a summary on the Jacobian of algebraic curves and its Néron model, which are indispensable to study the Galois representations associated with modular forms.

If we gave a proof of every single theorem or proposition in Chapters 1 and 2, it would become a whole book by itself. So, we only give proofs of important or simple properties. Please consider these chapters as a summary of known facts. Reading the chapters on elliptic curves and modular forms in *Number Theory 1,2, and 3* would also be useful to the reader.

At the end of the book, we give references for the theorems and propositions for which we could not give proofs in the main text. The interested reader can consult them for further information. We regret that we did not have room to mention the history of Fermat's Last Theorem. The reader can also refer to references at the end of the book. Due to the nature of this book, we did not cite the original paper of each theorem or proposition, and we beg the original authors for mercy.

I would be extremely gratified if more people could appreciate one of the highest achievements of the twentieth century in mathematics. I would like to express sincere gratitude to Professor Kazuya Kato for proposing that I write this book. I would also thank Masato Kurihara, Masato Kuwata, and Kazuhiro Fujiwara for useful advice. Also, particularly useful were the survey articles [**4**], [**5**], and [**24**]. I express here special thanks to their authors.

This book was based on lectures and talks at various places, including the lecture course at the University of Tokyo in the first semester of 1996, and intensive lecture courses at Tohoku University in May 1996, at Kanazawa University in September 1996, and at Nagoya University in May 1999. I would like to thank all those who attended these lectures and took notes. I would also like to thank former and current graduate students at the University of Tokyo, Keisuke Arai, Shin Hattori, and Naoki Imai, who read the earlier manuscript carefully and pointed out many mistakes. Most of the chapters up to Chapter 7 were written while I stayed at Université Paris-Nord, Max-Planck-Institut für Mathematik, and Universität Essen. I would like to thank these universities and the Institute for their hospitality and for giving me an excellent working environment.

This book is the combined edition of the two books in the Iwanami series The Development of Modern Mathematics: *Fermat's Last Theorem 1* first published in March 2000 and containing up to Chapter 7; and *Fermat's Last Theorem 2* published in February 2008.

Since 1994 when the proof was first published, the development of this subject has been remarkable: Conjecture 3.27 has been proved, and Conjecture 3.37 has almost been proved. Also, Theorem 5.22 has been generalized widely, and its proof has been simplified greatly. We should have rewritten many parts of this book to include recent developments, but we decided to wait until another opportunity arises.

On the occasion of the second edition, we made corrections to known errors. However, we believe there still remain many mistakes yet to be discovered. I apologize in advance, and would be grateful if the reader could inform me.

Takeshi Saito
Tokyo, Japan
November 2008

Preface to the English Edition

This is the second half of the English translation of *Fermat's Last Theorem* in the Iwanami series, The Development of Modern Mathematics. Though the translation is based on the second combined edition of the original Japanese book published in 2008, it will be published in two volumes. The first volume, *Fermat's Last Theorem: Basic Tools*, contains Chapters 0–7 and Appendix A. The second volume, *Fermat's Last Theorem: The Proof*, contains Chapters 8–11 and Appendices B, C, and D.

This second volume of the book on the proof of Fermat's Last Theorem by Wiles and Taylor presents a full account of the proof started in the first volume. As well as the proof itself, basic materials behind the proof, including the Galois representations associated with modular forms, the integral models of modular curves, the Hecke modules, the Selmer groups, etc., are studied in detail.

The author hopes that, through this edition, a wider audience of readers will appreciate one of the deepest achievements of the twentieth century in mathematics.

My special thanks are due to Dr. Masato Kuwata, who not only translated the Japanese edition into English but also suggested many improvements in the text so that the present English edition is more readable than the original Japanese edition.

Takeshi Saito
Tokyo, Japan
October 2014

CHAPTER 8

Modular curves over Z

In Chapter 2, we used modular curves over **Q** to define modular forms with **Q** coefficients. A modular curve over **Q** is the fiber over the generic point of a modular curve over **Z**. In this chapter we will define modular curves over **Z**, and prove their fundamental properties. In the next chapter we will derive various properties of Galois representations associated with modular forms by examining the properties of modular curves over **Z** at each prime number.

In §8.1, we classify elliptic curves in positive characteristics into ordinary elliptic curves and supersingular elliptic curves. We will define modular curves over **Z** using the Drinfeld level structure, which will be introduced in §8.3 after some preparations in §8.2. The Drinfeld level structure plays an important role when we study the structure of modular curves at a prime number dividing the level. In §8.5, we will define modular curves that play a complementary role, and we study reduction of these curves modulo p in §8.6. Using the results of §8.6, we will prove fundamental properties, Theorems 8.34 and 8.32 in §8.7 and §8.8, respectively. Since the modular curves defined in §8.4 are affine curves, we will compactify them and prove fundamental properties, Theorems 8.63 and 8.66, in §8.9.

8.1. Elliptic curves in characteristic $p > 0$

Let p be a prime number, let S be a scheme over $\mathbf{F}_p$, and let X be a scheme over S. Let $F_S : S \to S$ be the *absolute Frobenius morphism*, which is defined by the pth power mapping of the coordinate rings. We denote by $X^{(p)}$ the fiber product $X \times_S S$ by $F_S : S \to S$. The morphism $X \to X^{(p)}$ defined by the commutative diagram

$$\begin{tikzcd}
X \arrow[r, "F_X"] \arrow[d] & X \arrow[d] \\
S \arrow[r, "F_S"] & S
\end{tikzcd}$$

of the absolute Frobenius morphisms is denoted by F and is called the *relative Frobenius morphism*.

If $X = E$ is an elliptic curve, the morphism $F : E \to E^{(p)}$ is a morphism of elliptic curves over S of degree p. Let $V : E^{(p)} \to E$ be the dual morphism of $F : E \to E^{(p)}$. V is also a morphism of elliptic curves of degree p, and the compositions $V \circ F$ and $F \circ V$ are the multiplication-by-p mappings $[p] : E \to E$ and $[p] : E^{(p)} \to E^{(p)}$, respectively. For example, if $S = \operatorname{Spec} A$ and E is an elliptic curve given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, then $E^{(p)}$ is defined by the equation $y^2 + a_1^pxy + a_3^py = x^3 + a_2^px^2 + a_4^px + a_6^p$, and $F : E \to E^{(p)}$ is defined by $(x, y) \mapsto (x^p, y^p)$.

For a nonnegative integer e, we denote by $F^e : E \to E^{(p^e)}$ the composition of $F : E^{(p^i)} \to E^{(p^{i+1})}$, $i = 0, \ldots, e-1$, and let $V^e : E^{(p^e)} \to E$ be the dual of F^e.

DEFINITION 8.1. Let p be a prime number, let S be a scheme over $\mathbf{F}_p$, and let E be an elliptic curve over S.

(1) If $V : E^{(p)} \to E$ is étale, we say E is *ordinary*.
(2) If $E[p] = \operatorname{Ker} F^2$, we say E is *supersingular*.

A supersingular elliptic curve over a field is smooth and thus nonsingular. The term "supersingular" suggests it is very special in some sense. However, it is not directly related to the term "singular" in the sense that the local ring is not regular. Later in Theorem 8.32(4), we will prove that the points on the modular curve $Y_0(Mp)_{\mathbf{F}_p}$ $(p \nmid M)$ corresponding to supersingular elliptic curves coincide with the singular points of this modular curve. By Lemma 8.44, there exists an ordinary elliptic curve for each prime number p. We also prove that there exists a supersingular curve for each p in Corollary 8.64. We also calculate the number of isomorphism classes of supersingular elliptic curves over an algebraically closed field of characteristic $p > 0$.

Let p be a prime number, let S be a scheme over $\mathbf{F}_p$, and let E be an elliptic curve over S. Since the condition that $V : E^{(p)} \to E$ is étale is an open condition on S, the condition that E is ordinary is also an open condition. We denote by S^{ord} the maximal open subscheme U of S such that the restriction E_U is ordinary. Meanwhile, if we apply Corollary A.37(2) to $\operatorname{Ker} F^2$ and $E[p]$, the condition $\mathcal{P}$ that $E_T = E \times_S T$ is supersingular for an S-scheme T is a closed condition on S. We denote by S^{ss} the closed subscheme of S defined by the closed condition $\mathcal{P}$. We show that S^{ord} is the complementary open subscheme of S^{ss}. More precisely, we have the following.

PROPOSITION 8.2. *Let k be a field of characteristic $p > 0$, and let E be an elliptic curve over k. Let $\bar{k}$ be an algebraic closure of k. Then, the following hold.*

(1) *The order of the abelian group $E[p](\bar{k})$ is either p or 1.*
(2) *The following conditions* (i)–(iv) *are equivalent.*
  (i) *The order of the abelian group $E[p](\bar{k})$ is p.*
  (ii) *E is ordinary.*
  (iii) *For any integer $e \geq 1$, $\operatorname{Ker} V^e$ is étale and the abelian group $\operatorname{Ker} V^e(\bar{k})$ is isomorphic to $\mathbf{Z}/p^e\mathbf{Z}$.*
  (iv) *For any integer $e \geq 1$, the group scheme $E[p^e]_{\bar{k}}$ is isomorphic to $\mathbf{Z}/p^e\mathbf{Z} \times \mu_{p^e}$.*
(3) *The following conditions* (i)–(iii) *are equivalent.*
  (i) *The order of the abelian group $E[p](\bar{k})$ is 1.*
  (ii) *E is supersingular.*
  (iii) *For any integer $e \geq 1$, the only closed subgroup scheme of E of order p^e is $\operatorname{Ker} F^e$.*

PROOF. It suffices to prove the case where $k = \bar{k}$.

(1) As in Proposition 3.45, let $E[p]^0$ the connected component of $E[p]$ containing 0, and let $E[p]^{\text{ét}}$ be the maximal étale quotient. Consider the exact sequence

$$0 \longrightarrow E[p]^0 \longrightarrow E[p] \longrightarrow E[p]^{\text{ét}} \longrightarrow 0. \tag{8.1}$$

Since we assumed $k = \bar{k}$, the exact sequence (8.1) gives an isomorphism of finite groups $E[p](k) \to E[p]^{\text{ét}}(k)$. Consider the Cartier dual of (8.1). By the Weil pairing, the Cartier dual of $E[p]$ is $E[p]$ itself, and the Cartier dual of $E[p]^{\text{ét}}$ is connected. Thus, the Cartier dual $(E[p]^{\text{ét}})^\vee$ is a closed subgroup scheme of $E[p]^0$. Hence, $(\sharp E[p](k))^2 = (\deg E[p]^{\text{ét}})(\deg (E[p]^{\text{ét}})^\vee)$ divides $(\deg E[p]^{\text{ét}})(\deg E[p]^0) = \deg E[p] = p^2$.

(2) (i) $\Rightarrow$ (ii). Since $[p] = V \circ F$, we obtain the exact sequence

$$0 \longrightarrow \operatorname{Ker}(F : E \to E^{(p)}) \longrightarrow E[p] \xrightarrow{F} \operatorname{Ker}(V : E^{(p)} \to E) \longrightarrow 0. \tag{8.2}$$

Since $\operatorname{Ker} F(k) = 0$, $E[p](k) \to \operatorname{Ker} V(k)$ is an isomorphism of finite groups. By (i), the order of $\operatorname{Ker} V(k)$ is p, and thus the isogeny $V : E^{(p)} \to E$ of degree p is étale.

(ii) $\Rightarrow$ (iii). Since $V^e = V \circ V^{(p)} \circ \cdots \circ V^{(p^{e-1})}$, if V is étale, V^e is also étale of degree p^e. Thus, $\operatorname{Ker} V^e(k)$ is an abelian group of order p^e. Moreover, since the order of a p-torsion point of $\operatorname{Ker} V^e \subset E^{(p^e)}$ is p, $\operatorname{Ker} V^e$ is isomorphic to $\mathbf{Z}/p^e\mathbf{Z}$.

(iii) $\Rightarrow$ (iv). In the exact sequence

$$0 \to \operatorname{Ker}(F^e : E \to E^{(p^e)}) \longrightarrow E[p^e] \xrightarrow{F^e} \operatorname{Ker}(V^e : E^{(p^e)} \to E) \to 0, \tag{8.3}$$

$\operatorname{Ker} F^e$ is connected and $\operatorname{Ker} V^e$ is étale. Let $E[p^e]_{\mathrm{red}}$ be the reduced part of $E[p^e]$. Then, the composition $E[p^e]_{\mathrm{red}} \to E[p^e] \to \operatorname{Ker} V^e$ is an isomorphism since k is algebraically closed. Since $\operatorname{Ker} V^e$ is isomorphic to $\mathbf{Z}/p^e\mathbf{Z}$, $\operatorname{Ker} F^e$ is isomorphic to its Cartier dual μ_{p^e}.

(iv) $\Rightarrow$ (i). This is clear from $\mu_p(k) = \{1\}$.

(3) (i) $\Rightarrow$ (iii). If G is a closed subgroup scheme of $E[p^e]$ of degree p^e, then G is connected. Therefore, if $\mathfrak{m}_0$ is the maximal ideal of the local ring $\mathcal{O}_{E,0}$, we have $G = \operatorname{Spec} \mathcal{O}_{E,0}/\mathfrak{m}_0^{p^e} = \operatorname{Ker} F^e$.

(iii) $\Rightarrow$ (ii). Since $E[p]$ is a closed subgroup scheme of degree p^2, we have $E[p] = \operatorname{Ker} F^2$.

(ii) $\Rightarrow$ (i). We have $E[p](\bar{k}) = \operatorname{Ker} F^2(\bar{k}) = 0$. ☐

COROLLARY 8.3. *Let p be a prime number, let S be a scheme over $\mathbf{F}_p$, and let E be an elliptic curve over S. Then, we have*

$$S^{\mathrm{ord}} = S - S^{\mathrm{ss}}. \tag{8.4}$$

PROOF. It is clear from Proposition 8.2. ☐

LEMMA 8.4. *Let p be a prime number, let S be a scheme over $\mathbf{F}_p$, and let E be an elliptic curve over S. Let $e \geq 1$ be an integer.*

(1) *If E is ordinary, then $V^e : E^{(p^e)} \to E$ is étale, and* $\operatorname{Ker} V^e$ *is isomorphic to $\mathbf{Z}/p^e\mathbf{Z}$ étale locally.*
(2) *If $f : E \to E'$ is an étale isogeny of degree p^e, then both E and E' are ordinary, and there exists a unique isomorphism $g : E \to E'^{(p^e)}$ satisfying $f = V^e \circ g$.*

PROOF. (1) Similar to the proof of Proposition 8.2(2)(ii) $\Rightarrow$ (iii).

(2) Let ${}^t f : E' \to E$ be the dual of f. Since $f \circ {}^t f = [p^e]$, $\operatorname{Ker} {}^t f$ is an open and closed subgroup scheme of $E[p^e]$ of degree p^e, and its underlying set is equal to that of the 0-section of E'. Thus, $\operatorname{Ker} {}^t f$ is a closed subgroup scheme. Hence, we have $\operatorname{Ker} {}^t f = \operatorname{Ker} F^e$, and an isomorphism $g : E \to E'^{(p^e)}$ satisfying $F^e = g \circ {}^t f$ is induced. Clearly, g satisfies the required condition and g is unique.

Since $V^e : E'^{(p^e)} \to E'$ is étale, E' is ordinary. Moreover, since E and $E'^{(p^e)}$ are isomorphic, E is also ordinary. ☐

PROPOSITION 8.5. *Let p be a prime number, and let E be an elliptic curve over $\mathbf{F}_p$. Let $a = 1 + p - \sharp E(\mathbf{F}_p)$. Then, the following conditions* (i)–(iii) *are equivalent.*

(i) *E is ordinary.*
(ii) *$p \nmid a$.*
(iii) *If $p = 2$, $a = \pm 1$. If $p = 3$, $a = \pm 1, \pm 2$. If $p \geq 5$, $a \neq 0$.*

PROOF. As in Proposition 1.21, we have $1 - at + pt^2 = \det(1 - Ft : D(E))$ by Theorem C.1(4). By Proposition 8.2(2)(iv)$\Leftrightarrow$(ii) and Theorem C.1(2), E is ordinary if and only if one of the eigenvalues of the action of F on $D(E)$ is a p-adic unit. This is equivalent to condition (ii).

The equivalence of conditions (ii) and (iii) follows from the fact $|a| < 2\sqrt{p}$ and Theorem 1.15. □

EXAMPLE 8.6. Let p be an odd prime number, and let E be the elliptic curve over $\mathbf{F}_p$ given by $y^2 = x^3 - x$. Then, E is ordinary if $p \equiv 1 \bmod 4$, and E is supersingular if $p \equiv -1 \bmod 4$.

Indeed, since $E[2] = \{\infty, (0,0), (\pm 1, 0)\}$ is a subgroup of $E(\mathbf{F}_p)$, we have $\sharp E(\mathbf{F}_p) = p + 1 - a \equiv 0 \bmod 4$. Thus, if $p \equiv 1 \bmod 4$, we have $a \equiv 2 \bmod 4$, which means $a \neq 0$. If $p \equiv -1 \bmod 4$, then -1 is not a quadratic residue mod p. Hence, if $x \neq 0, \pm 1$, either $x^3 - x$ or $(-x)^3 - (-x) = -(x^3 - x)$ is a quadratic residue, and not both. Thus, we have $\sharp E(\mathbf{F}_p) = p + 1$, which means $a = 0$.

Similarly, for a prime number $p \geq 5$, let E be the elliptic curve over $\mathbf{F}_p$ defined by $y^2 = x^3 - 1$. Then, E is ordinary if $p \equiv 1 \bmod 3$, and its supersingular if $p \equiv -1 \bmod 3$.

COROLLARY 8.7. *Let p be an odd prime number, and let E be an elliptic curve over $\mathbf{Q}_p$. Then the following conditions* (i) *and* (ii) *are equivalent.*

(i) *The p-adic representation V_pE of $G_{\mathbf{Q}_p}$ is ordinary.*
(ii) *Either E has good reduction and $E_{\mathbf{F}_p}$ is ordinary or E has multiplicative reduction.*

PROOF. First, we assume E has good reduction, and we show V_pE is ordinary if and only if $E_{\mathbf{F}_p}$ is ordinary. By Theorem C.6(3), the subspace $D'(E) \subset D(E)$ is one dimensional. Thus, by Corollary C.8, V_pE is ordinary if and only if there exist p-adic units α and β such that $1 - at + pt^2 = \deg(1 - Ft : D(E))$ decomposes into $(1 - \alpha t)(1 - p\beta t)$. This is in turn equivalent to that $E_{\mathbf{F}_p}$ is ordinary by Proposition 8.5.

Furthermore, by Proposition 3.46(2), E has stable reduction if V_pE is ordinary. This shows (i)⇒(ii).

Suppose E has multiplicative reduction. In this case, we have already proved that V_pE is ordinary in the proof of Proposition 3.46(2) (i)⇒(ii). This shows (ii)⇒(i). □

8.2. Cyclic group schemes

In this section we define cyclic group scheme as a preparation for the definition of modular curves over **Z**.

DEFINITION 8.8. Let S be a scheme, let $N \geq 1$ be an integer, and let X be a finite flat scheme of finite presentation over S of degree N. A family of sections $P_1, \ldots, P_N : S \to X$ is called a *full set of sections of X* if it satisfies

$$N_{X_R/R}(f) = \prod_{i=1}^{N} f(P_i) \tag{8.5}$$

for any commutative ring R, any morphism $\operatorname{Spec} R \to S$, and any element $f \in \Gamma(X \times_S \operatorname{Spec} R, \mathcal{O})$.

LEMMA 8.9. *Let S be a scheme, let $N \geq 1$ be an integer, and let X be a finite flat scheme of finite presentation over S of degree N. If a family of sections $P_1, \ldots, P_N : S \to X$ is a full set of sections, the morphism*

$$\coprod_{i=1}^{N} P_i : S \coprod \cdots \coprod S \to X \tag{8.6}$$

is surjective.

PROOF. It suffices to show it when $S = \operatorname{Spec} k$, where k is an algebraically closed field, but it is clear in this case. □

Even if the morphism (8.6) is surjective, $P_1, \ldots, P_N$ may not be a full set of sections of X. For example, let k be a field, let $S = \operatorname{Spec} k[\epsilon]/(\epsilon^2)$, and let $X = \operatorname{Spec} k[\epsilon, \epsilon'](\epsilon^2, \epsilon'^2)$. Define sections $P_1, P_2 : S \to X$ by $\epsilon \mapsto 0$ and $\epsilon' \mapsto \epsilon$, respectively. Then, $P_1 \coprod P_2 : S \coprod S \to X$ is surjective. However, if we let $f = 1 + \epsilon'$, we have $N_{X/S}(f) = 1 \neq f(P_1)f(P_2) = 1 + \epsilon$. This means P_1 and P_2 do not form a full set of sections of X.

If X is étale, the condition in Lemma 8.9 is a necessary and sufficient condition.

COROLLARY 8.10. *If X is étale over S in Lemma 8.9, then the following conditions are equivalent.*

(i) $P_1, \dots, P_N : S \to X$ *form a full set of sections of* X.

(ii) $\coprod_{i=1}^{N} P_i : S \coprod \cdots \coprod S \to X$ *is an isomorphism.*

(iii) $\coprod_{i=1}^{N} P_i : S \coprod \cdots \coprod S \to X$ *is surjective.*

PROOF. (ii) ⇒ (i) is clear. (i) ⇒ (iii) holds by Lemma 8.9. Since $S \coprod \cdots \coprod S$ and X are both finite étale of degree N, (ii) and (iii) are equivalent. ☐

PROPOSITION 8.11. *Let S be a scheme, let $N \geq 1$ be an integer, and let X be a finite flat scheme of finite presentation over S of degree N. Let $P_1, \dots, P_N : S \to X$ be a family of sections of X. The condition $\mathcal{P}$ that $P_1, \dots, P_N$ form a full set of sections of X is a closed condition on S. The ideal of $\mathcal{O}_S$ that defines the closed subscheme T of S defined by the closed condition $\mathcal{P}$ is locally of finite type.*

PROOF. Since the assertion is local on S, it suffices to show the cases where $S = \operatorname{Spec} A$ and $X = \operatorname{Spec} B$ with B a free A-module of rank N. Let $g_1, \dots, g_N$ be a basis of the A-module B. The equality (8.5) holds for any R and f if and only if (8.5) holds for the polynomial ring $R = A[T_1, \dots, T_N]$ and $f = \sum_{j=1}^{N} g_j T_j \in B[T_1, \dots, T_N]$. For such R and f, (8.5) becomes

$$N_{B[T_1,\dots,T_N]/A[T_1,\dots,T_N]}\Big(\sum_{j=1}^{N} g_j T_j\Big) = \prod_{i=1}^{N}\Big(\sum_{j=1}^{N} g_j(P_i) T_j\Big). \tag{8.7}$$

If $I \subset A$ is the ideal generated by the coefficients of the difference of the both sides of (8.7), the closed subscheme T of S defined by I represents the functor $F_{\mathcal{P}}$. Since each side of (8.7) is a homogeneous polynomial of degree N in $T_1, \dots, T_N$ with A coefficients, I is finitely generated. ☐

If X is a closed subscheme of a smooth curve, we have the proposition below. Note that if E is a smooth curve over S and X is a closed subscheme of E that is finite flat of finite presentation over S, then X is a Cartier divisor of E by Lemma B.2(1). In particular, a section $P : S \to E$ defines a Cartier divisor of E.

PROPOSITION 8.12. *Let S be a scheme, let E be a smooth curve over S, and let $N \geq 1$ be an integer. Suppose X is a closed subscheme of E that is finite flat of finite presentation over S of degree N. For sections $P_1, \dots, P_N : S \to X$, the following are equivalent.*

(1) *$P_1, \ldots, P_N$ form a full set of sections of X.*
(2) *The following equality of Cartier divisors holds:*

$$X = \sum_{i=1}^{N} [P_i].$$

PROOF. (ii) $\Rightarrow$ (i). Let $\operatorname{Spec} R \to S$ be a morphism of schemes. We show $N_{X_R/R}(f) = \prod_{i=1}^N f(P_i)$ for $f \in \Gamma(X_R, \mathcal{O})$. Replacing S by $\operatorname{Spec} R$, we may assume $S = \operatorname{Spec} R$. For $i = 1, \ldots, N$, let $\mathcal{I}_i$ be the defining ideal sheaf of the Cartier divisor $[P_i]$ of E. By the equality of divisors $X = \sum_{i=1}^N [P_i]$, the finitely generated free $\mathcal{O}_S$-module $\mathcal{O}_X$ is a successive extension of the invertible $\mathcal{O}_S$-modules $\prod_{j=1}^{i-1} \mathcal{I}_j / \prod_{j=1}^{i} \mathcal{I}_j$. Since the multiplication-by-f map of $\mathcal{O}_X$ induces the multiplication-by-$f(P_i)$ map of $\prod_{j=1}^{i-1} \mathcal{I}_j / \prod_{j=1}^{i} \mathcal{I}_j$, we have $N_{X/S}(f) = \prod_{i=1}^N f(P_i)$.

(i) $\Rightarrow$ (ii). Both X and $\sum_{i=1}^N [P_i]$ are finite flat of finite presentation over S of degree N. Thus, it suffices to show X is a closed subscheme of $\sum_{i=1}^N [P_i]$. Let $s \in S$. We may replace S by $\operatorname{Spec} \mathcal{O}_{S,s}$. By Lemma 8.9, we have $X = \bigcup_{i=1}^N P_i(S)$. Since $A = \mathcal{O}_{S,s}$ is a local ring, $P_i(s) \neq P_j(s)$ implies $P_i(S) \cap P_j(S) = \varnothing$ for $i, j = 1, \ldots, N$. Thus $X = \coprod_{x \mapsto s} \bigcup_{P_i(s)=x} P_i(S)$. Hence, for an inverse image x of s, we have $\operatorname{Spec} \mathcal{O}_{X,x} = \bigcup_{P_i(s)=x} P_i(S)$ and $X = \coprod_{x \mapsto s} \operatorname{Spec} \mathcal{O}_{X,x}$. Therefore, it suffices to show the assertion assuming $X = \operatorname{Spec} \mathcal{O}_{X,x}$. Replacing E by an open neighborhood of x, we may assume E is also affine.

Let $E = \operatorname{Spec} B$ and $X = \operatorname{Spec} \overline{B}$. Replacing E by an open neighborhood of x again if necessary, we may assume the divisor $[P_1]$ of E is defined at $t \in B$. For $i = 2, \ldots, N$, $t - t(P_i) \in B$ is also 0 on P_i. Since the divisor $[x] = [P_i(s)]$ of E_s is defined by $t - t(P_i)$ on a neighborhood of x, it follows from Nakayama's lemma that a divisor $[P_i]$ of E is defined by $t - t(P_i) \in B$ on a neighborhood of x. Replacing E once again by an open neighborhood of x if necessary, we may assume the divisor $[P_i]$ of E is defined by $t - t(P_i) \in B$ for $i = 1, \ldots, N$.

Let $\Phi(T) = N_{\overline{B}/A}(T - t|_X) \in A[T]$. Applying (8.5) to $f = T - t \in B \otimes_A A[T]$, we obtain $\Phi(T) = \prod_{i=1}^N (T - t(P_i))$. Thus, $\Phi(t) = \prod_{i=1}^N (t - t(P_i)) \in B$ is a generator of the defining ideal of the divisor $\sum_{i=1}^N [P_i]$ of E. On the other hand, by the theorem of Cayley and Hamilton, $\Phi(t|_X) \in \overline{B}$ is 0. Thus, $\Phi(t) \in B$ is contained in the defining ideal $\mathrm{Ker}(B \to \overline{B})$ of X. This shows that X is a closed subscheme of $\sum_{i=1}^{N}[P_i]$ at each point of X. □

DEFINITION 8.13. Let S be a scheme, let $N \geq 1$ be an integer, and let G be a finite flat commutative group scheme of finite presentation over S of degree N.

(1) Let $P : S \to G$ be a section of G. If the family 0, P, $2P, \dots,$ $(N-1)P$ is a full set of sections, we call P a *generator* of G.
(2) G is called a *cyclic group scheme* if there exists a generator of G flat locally on S.

The degree of a cyclic group scheme is sometimes called the order. If N is invertible on S, Lemma 8.15 below shows this coincides with the ordinary definition. We show the following proposition first.

PROPOSITION 8.14. *Let S be a scheme, and let G be a finite flat commutative group scheme of finite presentation of degree M. Then, the multiplication-by-M mapping of G is the 0 mapping.*

PROOF. It suffices to show $g^M = 1$ for any scheme T over S and any section $g \in G(T)$. Replacing S by T, we may assume $S = T$. Since the assertion is local on S, we may assume $S = \operatorname{Spec} R$, $G = \operatorname{Spec} A$, and A is a free R-module of rank M. Let $G^\vee = \operatorname{Spec} A^\vee$, where $A^\vee = \mathrm{Hom}_R(A, R)$, be the Cartier dual of G. The multiplication of $A^\vee$ is the dual of the ring morphism $A \to A \otimes_R A$ that defines the group operation $\mu : G \times_S G \to G$.

Let $g \in G(S)$, let $\mu_g : G \to G$ be the translation by g, and let $\mu_g : A \to A$ be the corresponding isomorphism of rings. We identify $g \in G(S) = \mathrm{Hom}_{R\text{-alg}}(A, R) \subset \mathrm{Hom}_R(A, R)$ with an element of $A^\vee = \mathrm{Hom}_R(A, R)$. Furthermore, we identify $\mu_g \in G(G) = \mathrm{Hom}_{R\text{-alg}}(A, A) \subset \mathrm{End}_R A$ with an element of $\mathrm{End}_R A = A \otimes_R A^\vee$. Since $G(G)$ is a subgroup of $(A \otimes_R A^\vee)^\times$, $\mu_g \in A \otimes_R A^\vee$ is invertible. Moreover, since $\mu_g : G \to G$ is the product of $\mathrm{id} = \mu_1 : G \to G$ and $G \to S \xrightarrow{g} G$, we have $\mu_g = \mu_1 \cdot (1 \otimes g) \in A \otimes_R A^\vee$. Thus, taking the norm $N = N_{A \otimes_R A^\vee / A^\vee}$ of both sides, we obtain $N(\mu_g) = N(\mu_1) \cdot g^M \in A^{\vee\times}$. On the other hand, since $\mu_g(\mu_1) = \mu_1 \circ \mu_g = \mu_g$, the homomorphism of $A^\vee$-algebras $(\mu_g \otimes 1) : A \otimes_R A^\vee \to A \otimes_R A^\vee$ maps μ_1 to μ_g. Thus, we have $N(\mu_g) = N(\mu_1) \in A^{\vee\times}$. This shows $g^M = 1 \in G(S) \subset A^\vee$. □

LEMMA 8.15. *Let S be a scheme, let $N \geq 1$ be an integer invertible on S, and let G be a finite flat commutative group scheme of finite presentation over S of degree N.*

(1) *For a section $P : G \to S$, the following are equivalent.*
   (i) *P is a generator of G.*
   (ii) *For any geometric point $\bar{s}$ in S, $P_{\bar{s}} \in G(\bar{s})$ is a generator of $G(\bar{s})$.*
   (iii) *There exists an isomorphism of commutative group schemes $\mathbf{Z}/N\mathbf{Z} \to G$ that maps 1 to P.*
(2) *The following are equivalent.*
   (i) *G is a cyclic group scheme.*
   (ii) *For any geometric point $\bar{s}$ in S, $G(\bar{s})$ is a cyclic group.*
   (iii) *There exits an isomorphism of commutative group schemes $\mathbf{Z}/N\mathbf{Z} \to G$ étale locally on S.*

PROOF. Since G is étale over S by Proposition 8.14 and Definition A.17, the assertions are clear from Corollary 8.10. ☐

LEMMA 8.16. *Let S be a scheme, let $N \geq 1$ be an integer, and let G be a finite flat commutative group scheme over S of finite presentation of degree N.*

(1) *Let $P : S \to G$ be a section of D. The condition that P is a generator of G is a closed condition on S. The ideal of $\mathcal{O}_S$ defining the closed subscheme T of S defined by this condition is locally of finite type.*
(2) *The functor that associates the set*

$$\{P \in G(T) \mid P \text{ is a generator of } G_T\} \tag{8.8}$$

to a scheme T over S is represented by a closed subgroup scheme $G^\times$ of G.

PROOF. (1) It suffices to apply Proposition 8.11 to the sections $0, P, \ldots, (N-1)P$ of G.

(2) It suffices to apply (1) to the pullback section of G to G defined by the diagonal map $G \to G \times_S G$. ☐

The closed subgroup scheme $G^\times$ of G is called the *scheme of generators* of G. If $G^\times$ is faithfully flat over S, then $G^\times$ is a flat covering of S, and thus G is a cyclic group scheme. Later in Corollary 8.53(1), we will show a partial converse of this property.

LEMMA 8.17. *Let S be a scheme, let $0 \to G' \to G \to G'' \to 0$ be an exact sequence of finite flat commutative group schemes of finite* *presentation over S, and let P be a section of G. Suppose G'' is étale of degree M. Then, the following are equivalent.*

(i) *P is a generator of G.*

(ii) *The image P'' of P is a generator of G'', and MP is a generator of G'.*

PROOF. (i) ⇒ (ii). Let P be a generator of G, and let N be the degree of G. By Lemma 8.9, $\coprod_{i=0}^{N-1} iP : S \coprod \cdots \coprod S \to G \to G''$ is surjective. Thus, by Proposition 8.14, $\coprod_{i=0}^{N-1} iP'' : S \coprod \cdots \coprod S \to G''$ is also surjective. Therefore, by Corollary 8.10, P'' defines an isomorphism $\mathbf{Z}/M\mathbf{Z} \to G''$, and P'' is a generator of G''. Moreover, since $\coprod_{i=0}^{M-1}(+iP) : \coprod_{i=0}^{M-1} G' \to G$ is an isomorphism of schemes, P is a generator of G if and only if MP is a generator of G''.

(ii) ⇒ (i). P'' defines an isomorphism $\mathbf{Z}/M\mathbf{Z} \to G''$, by Corollary 8.10. The remaining part is similar to the proof of (i) ⇒ (ii). □

LEMMA 8.18. *Let S be a scheme, and let E be a commutative group scheme over S that is a smooth curve over S. Let $N \geq 1$ be an integer.*

(1) *Let $P : S \to E$ be a section of E. Then, the following are equivalent.*
    (i) *There exists a closed subgroup scheme of E of order N such that P is its generator.*
    (ii) *The Cartier divisor $\sum_{i=0}^{N-1}[iP]$ of E is a closed subgroup scheme of E.*

(2) *If one of the equivalent conditions of (1) holds, then $NP = 0$, and $G = \sum_{i=0}^{N-1}[iP]$.*

(3) *Let G be a closed subgroup scheme of E finite flat of finite presentation of degree N over S. Let P be a section of E over G defined by the diagonal map $G \to E \times_S G$. The scheme $G^\times$ of generators of G is a closed subscheme defined by the closed condition on G that for any scheme T over G, the two closed subschemes of E_T, G_T and $\sum_{i=0}^{N-1}[iP]_T$ are equal.*

PROOF. (1) Clear from Proposition 8.12.

(2) Since the cyclic subgroup scheme $\sum_{i=0}^{N-1}[iP]$ is a finite flat commutative group scheme of finite presentation of degree N, the image of the multiplication-by-N map of $\sum_{i=0}^{N-1}[iP]$ is 0 by Proposition 8.14. Thus, we have $NP = 0$. $G = \sum_{i=0}^{N-1}[iP]$ is clear from Proposition 8.12.

(3) Clear from (2). □

LEMMA 8.19. *Let $N \geq 1$ be an integer. The group scheme $\mu_N = \operatorname{Spec} \mathbf{Z}[X]/(X^N - 1)$ consisting of Nth roots of unity is a cyclic group scheme. If $\Phi_N(X) \in \mathbf{Z}[X]$ is the Nth cyclotomic polynomial, the scheme $\mu_N^\times$ of generators of μ_N is* $\operatorname{Spec} \mathbf{Z}[X]/(\Phi_N(X))$.

PROOF. $\operatorname{Spec} \mathbf{Z}[X]/(\Phi_N(X))$ is a flat covering of $\operatorname{Spec} \mathbf{Z}$. Thus, if we show $\mu_N^\times = \operatorname{Spec} \mathbf{Z}[X]/(\Phi_N(X))$, then it follows that μ_N is a cyclic group scheme. Clearly, $\mu^\times_{N,\operatorname{Spec} \mathbf{Z}[\frac{1}{N}]} = \operatorname{Spec} \mathbf{Z}[\frac{1}{N}][X]/(\Phi_N(X))$ over $\operatorname{Spec} \mathbf{Z}[\frac{1}{N}]$ by Lemma 8.15. Thus, applying Corollary A.44(1) to $S = \operatorname{Spec} \mathbf{Z}$, $X = \mathbf{G}_{m,S}$, $A = \mu^\times_{N,S}$, and $B = \operatorname{Spec} \mathbf{Z}[X]/(\Phi_N(X))$, it suffices to show the inequality $\deg \mu^\times_{N,k} \leq \varphi(N)$ for any algebraically closed field k. By Lemma 8.17, it suffices to show the case where the characteristic of k is $p > 0$ and $N = p^e$.

By changing coordinates, let $\mathbf{G}_m = \operatorname{Spec} k[X, (1+X)^{-1}]$ and $G = \mu_N = \operatorname{Spec} k[X]/(X^N)$. Let $P : G \to \mathbf{G}_m \times_k G$ be the diagonal section. By Lemma 8.18(3), the closed subscheme $G^\times$ of G is defined by the closed condition that the two closed subschemes of $\mathbf{G}_m \times_k G = \operatorname{Spec} k[X, (1+X)^{-1}, T]/(T^N)$, $G \times_k G = \operatorname{Spec} k[X, T]/(X^N, T^N)$ and the pullback of

$$\sum_{i=0}^{N-1} [iP] = \operatorname{Spec} k[X, (1+X)^{-1}, T] \Big/ \left(\prod_{i=0}^{N-1} (1 + X - (1+T)^i), T^N \right)$$

are equal. Thus, if we let

$$\prod_{i=0}^{N-1} \left(1 + X - (1+T)^i\right) = X^N - \sum_{j=0}^{N-1} a_j(T) X^j,$$

we have $G^\times = \operatorname{Spec} k[T]/(T^N, a_0(T), \ldots, a_{N-1}(T))$. Since we have $(1+T)^i - 1 \equiv iT \bmod T^2$, the T-adic valuation $\operatorname{ord}((1+T)^i - 1)$ is 1 if $p \nmid i$, and at least 2 if $p \mid i$. Thus, we have $\operatorname{ord} a_{N/p}(T) = \sharp\{i \mid p \nmid i, 0 \leq i < N\} = N - N/p = \varphi(N)$, and we have $\deg G^\times = \min(N, \operatorname{ord} a_0(T), \ldots, \operatorname{ord} a_{N-1}(T)) \leq \varphi(N)$. □

8.3. Drinfeld level structure

In Chapter 2, we defined modular curves over **Q** using a cyclic subgroup of order N of an elliptic curve. However, for a supersingular elliptic curve over a scheme over $\mathbf{F}_p$, there is no cyclic subgroup scheme of order p in a usual sense. In order to define modular curves over **Z**, we use Definition 8.13 as the definition of a cyclic subgroup scheme. The level structure defined in such a way is called the *Drinfeld level structure*.

DEFINITION 8.20. Let S be a scheme, and let E be a commutative group scheme over S that is a smooth curve over S. Let $N \geq 1$ be an integer.

(1) A section $P : S \to E$ has *exact order* N if the Cartier divisor $\sum_{i=0}^{N-1}[iP]$ is a closed subgroup scheme of E. If P has exact order N, we call

$$\langle P \rangle = \sum_{i \in \mathbf{Z}/N\mathbf{Z}} [iP] \tag{8.9}$$

the cyclic subgroup scheme of order N generated by P.

(2) The functor $\mathcal{M}_0(N)_E$ over S is defined by associating to a scheme T over S the set

$$\mathcal{M}_0(N)_E(T) = \{\text{cyclic subgroup scheme of } E_T \text{ of order } N\}. \tag{8.10}$$

(3) The functor $\mathcal{M}_1(N)_E$ over S is defined by associating to a scheme T over S the set

$$\mathcal{M}_1(N)_E(T) = \{\text{section of } E_T \text{ of exact order } N\}. \tag{8.11}$$

By Lemma 8.18, the cyclic subgroup scheme in Definition 8.20(1) is a cyclic group scheme in the sense of Definition 8.13(2).

To a section $P \in \mathcal{M}_1(N)_E(T)$ of exact order N, associate the cyclic subgroup scheme $\langle P \rangle \in \mathcal{M}_0(N)_E(T)$, and we obtain a natural morphism of functors $\mathcal{M}_1(N)_E \to \mathcal{M}_0(N)_E$.

If N is invertible on S, Definition 8.20 is a standard one.

LEMMA 8.21. *Let S be a scheme, and let E be a commutative group scheme over S that is a smooth curve over S. Let $P : S \to E$ be a section of E, and let $N \geq 1$ be an integer.*

If N is invertible on S, the following conditions (i)–(iii) *are equivalent.*

(i) *P has exact order N.*

(ii) *There exists a closed immersion $\mathbf{Z}/N\mathbf{Z} \to E$ of commutative group schemes over S such that $P : S \to E$ is defined by $1 \in \mathbf{Z}/N\mathbf{Z}$.*

(iii) *$NP = 0$, and for any geometric point $\bar{s}$ in S, the element $P_{\bar{s}}$ of the abelian group $E(\bar{s})$ has exact order N.*

PROOF. Clear from Lemmas 8.18(2) and 8.15. ☐

For a scheme over $\mathbf{F}_p$ unusual phenomena occur unlike schemes over $\mathbf{Q}$.

LEMMA 8.22. *Let S be a scheme, and let E be a commutative group scheme over S that is a smooth curve over S. Let p be a prime number, and let $e \geq 1$ be an integer. Then, the following conditions* (i)–(iii) *are equivalent.*

(i) *S is a scheme over $\mathbf{F}_p$.*
(ii) *The 0-section of E has exact order p^e.*
(iii) *The Cartier divisor $G = p^e[0]$ of E is a cyclic subgroup scheme of order p^e.*

If one and hence all of these conditions hold, we have $G = \operatorname{Ker} F^e$.

PROOF. (i) $\Rightarrow$ (ii), (iii). If S is a scheme over $\mathbf{F}_p$, $p^e[0] = \operatorname{Ker} F^e$ is a cyclic subgroup scheme of order p^e, and the 0-section has exact order p^e.

(ii) $\Rightarrow$ (iii) is clear.

(iii) $\Rightarrow$ (i). Since the assertion is local on S, we may assume $S = \operatorname{Spec} A$. Furthermore, we may assume that the Cartier divisor $[0]$ of E is defined by a section T of $\mathcal{O}_E$ on a neighborhood of $[0]$. Then, we have $G = \operatorname{Spec} A[T]/(T^{p^e})$. Let $F(T,S)$ be the image of T by the ring homomorphism $A[T]/(T^{p^e}) \to A[T]/(T^{p^e}) \otimes_A A[T]/(T^{p^e}) = A[T,S]/(T^{p^e}, S^{p^e})$ corresponding to the group operation $G \times G \to G$. Here, we identify $T = T \otimes 1$, and let $S = 1 \otimes T$.

$F(T,S)^{p^e}$ equals 0 as an element of $A[T,S]/(T^{p^e}, S^{p^e})$. Since $F(T,0) = F(0,T) = T$, there exists $f(S,T) \in A[T,S]/(T^{p^e}, S^{p^e})$ such that $F(T,S) = T + S + STf(S,T)$. Looking at the homogeneous degree p^e part of $F(T,S)^{p^e}$, all the coefficients of $(T+S)^{p^e} - (T^{p^e} + S^{p^e}) = \sum_{i=1}^{p^e-1} \binom{p^e}{i} T^{p^e-i} S^i$ are 0 as elements of A. Since the greatest common divisor of $\binom{p^e}{1}$ and $\binom{p^e}{p^e-1}$ is p, A is an $\mathbf{F}_p$-algebra. $\square$

LEMMA 8.23. *Let S be a scheme, and let E be a commutative group scheme over S that is a smooth curve over S. Let $N \geq 1$ be an integer, and let $P : S \to E$ be a section of E. For a scheme T over S, the condition $\mathcal{P}$ that P_T is a section of exact order N of E_T is a closed condition on S.*

PROOF. Let $G = \sum_{i=0}^{N-1} [iP]$. By Definition 8.20(1), the condition $\mathcal{P}$ is that G_T is a closed subgroup scheme of E_T. This condition is in turn equivalent to the following. The closed subscheme $G_T \times_T G_T$

of $E_T \times_T E_T$ is a closed subscheme of the inverse image of G_T by the addition $+ : E_T \times_T E_T$, and G_T is equal to the inverse image of G_T by the multiplication-by-(-1) morphism $E_T \to E_T$. Thus, by Corollary A.37, the condition $\mathcal{P}$ is a closed condition. □

COROLLARY 8.24. *Let S be a scheme, and let E be an elliptic curve over S. Let $N \geq 1$ be an integer. The functor $\mathcal{M}_1(N)_E$ over S is represented by a scheme $M_1(N)_E$ finite of finite presentation over S. If N is invertible on S, $M_1(N)_E$ is étale over S.*

PROOF. Applying Lemma 8.23 to the diagonal section $E[N] \to E \times_S E[N]$ over $E[N]$, $\mathcal{M}_1(N)_E$ is represented by a closed subscheme of $E[N]$. If N is invertible on S, $E[N]$ is finite étale over S by Corollary 1.27. Since the assertion is étale local on S, we may assume that $E[N]$ is isomorphic to the constant group scheme $(\mathbf{Z}/N\mathbf{Z})^2$. But, in this case $\mathcal{M}_1(N)_E$ is isomorphic to $\coprod_{a \in (\mathbf{Z}/N\mathbf{Z})^n, \mathrm{ord}(a)=N} S$. □

LEMMA 8.25. *Let k be a field of characteristic p, and let E be an elliptic curve over k. Let $N \geq 1$ be an integer.*

(1) *If $p > 0$ and G is a closed subgroup scheme of E of degree p^e, then G is a cyclic subgroup scheme of order p^e.*

(2) *If G is a cyclic subgroup scheme of E of order N, then we have*

$$\deg G^\times \leq \varphi(N). \tag{8.12}$$

The equality holds unless $p \mid N$ and E is supersingular.

(3) *We have an equality*

$$\deg M_1(N)_E = \varphi(N)\psi(N) \tag{8.13}$$

unless $p \mid N$ and E is supersingular.

Later in Proposition 8.52 and Corollary 8.53, we will show that the equality holds even if E is supersingular.

QUESTION. In case $p \mid N$ and E is supersingular, can we prove directly the equality (8.12) as in the proof below?

PROOF. We may assume k is algebraically closed.

(1) If E is supersingular, a closed subgroup scheme of degree p^e is $\operatorname{Ker} F^e$ by Proposition 8.2(3), and 0 is a generator of this.

If E is ordinary, $E[p^e]$ is isomorphic to $\mathbf{Z}/p^e\mathbf{Z} \times \mu_{p^e}$ by Proposition 8.2(2). Let G be a closed subgroup scheme of $E[p^e]$ of degree p^e. Since $G \cap \mu_{p^e}$ is a closed subgroup scheme of μ_{p^e}, we have $G \cap \mu_{p^e} = \mu_{p^b}$ for some $b \geq e$. Since k is algebraically closed, G is isomorphic to $\mathbf{Z}/p^a\mathbf{Z} \times \mu_{p^b}$, $a + b = e$. By Lemma 8.17, $(1, 1)$ is a generator of $\mathbf{Z}/p^a\mathbf{Z} \times \mu_{p^b}$, and this is a cyclic subgroup scheme.

(2) By Lemma 8.17 it suffices to show it when $p > 0$ and $N = p^e$.

We show inequality (8.12) when E is supersingular. The proof goes similarly to that of Lemma 8.19. By Proposition 8.2(3), we have $G = \operatorname{Ker} F^e$. Choosing an isomorphism $k[[X]] \to \widehat{\mathcal{O}}_{E,0}$, we identify $k[[X]] = \widehat{\mathcal{O}}_{E,0}$. Then, we have $G = \operatorname{Spec} k[[X]]/(X^N)$. For an integer i, we denote by $[i]^*$ the ring homomorphism $k[[X]] \to k[[X]]$ induced by the multiplication-by-i mapping $[i] : E \to E$. $G^\times$ is a closed subscheme of $G = \operatorname{Spec} k[T]/(T^N)$ defined by the condition that the ideal $(\prod_{i=0}^{N-1}(X - [i]^*T))$ is equal to the ideal (X^N), and we have $[i]^*(T) \equiv iT \bmod T^2$. After this point, the proof goes in the same way as the proof of Lemma 8.19.

We show the equality in (8.12) when E is ordinary. By the proof of (1), we may assume $G = \mathbf{Z}/p^a \times \mu_{p^b}$, $a + b = e$. If $a = 0$, then the equality follows from Lemma 8.19. Suppose $a > 0$. By Lemma 8.17, a section P of $G = \mathbf{Z}/p^a\mathbf{Z} \times \mu_{p^b}$ is a generator if and only if the projection of P to $\mathbf{Z}/p^a\mathbf{Z}$ is a generator of $\mathbf{Z}/p^a\mathbf{Z}$ and p^aP is a generator of μ_{p^b}. By the assumption $a > 0$ and Lemma 8.19, p^aP is a generator of μ_{p^b} for any P. Thus, $G^\times$ is equal to $(\mathbf{Z}/p^a\mathbf{Z})^\times \times \mu_{p^b}$, and the equality holds.

(3) By Lemma 8.17, it suffices to show it when $p > 0$ and $N = p^e$. Suppose E is ordinary, and we show (8.13). As above, we may identify $E[N]$ with $G = \mathbf{Z}/N\mathbf{Z} \times \mu_N$. $M_1(N)_E$ is the closed subgroup scheme consisting of all the sections of G of exact order N. Decompose $G = \coprod_{i\in\mathbf{Z}/N\mathbf{Z}} G^i = \coprod_{i\in\mathbf{Z}/N\mathbf{Z}} \mu_N$, and $M_1(N)_E = \coprod_{i\in\mathbf{Z}/N\mathbf{Z}} M_1(N)_E^i$. If $i \in \mathbf{Z}/N\mathbf{Z}$ has order p^a, and $a \leq e = a + b$, then by Lemma 8.17, $M_1(N)_E^i$ is the inverse image of $\mu_{p^b}^\times$ by the multiplication-by-p^a mapping $G^i = \mu_{p^e} \to \mu_{p^b}$. Thus, $M_1(N)_E^i = \mu_{p^e}^\times$ if $b > 0$, and $M_1(N)_E^i = G^i$ if $b = 0$. The equality (8.13) is clear. □

As a preparation for studying the compactification of modular curves in §8.9, we define and study the Drinfeld level structure of a commutative group scheme. Let $N \geq 1$ be an integer. Define a morphism $\mathbf{Z} \to \mathbf{Z} \times \mathbf{G}_m$ of commutative group schemes over $\mathbf{Z}[q, q^{-1}]$ by sending 1 to (N, q), and define $T^{(N)}$ to be the cokernel of this homomorphism. $T^{(N)}$ is an extension of $\mathbf{Z}/N\mathbf{Z}$ by $\mathbf{G}_m$, and the kernel $T[N]$ of the multiplication-by-N map $T^{(N)} \to T^{(N)}$ is an extension of $\mathbf{Z}/N\mathbf{Z}$ by μ_N. For $i \in \mathbf{Z}/N\mathbf{Z}$, let $T^{(N)i}$ and $T[N]^i$ be the inverse images of the natural morphisms to $\mathbf{Z}/N\mathbf{Z}$. We have

$$T^{(N)} = \coprod_{i=0}^{N-1} T^{(N)i} = \coprod_{i=0}^{N-1} \operatorname{Spec} \mathbf{Z}[q, q^{-1}][T, T^{-1}]$$

and

$$T[N] = \coprod_{i=0}^{N-1} T[N]^i = \coprod_{i=0}^{N-1} \operatorname{Spec} \mathbf{Z}[q, q^{-1}][T]/(T^N - q^i). \tag{8.14}$$

PROPOSITION 8.26. *Let $N \geq 1$ be an integer.*

(1) *The functor $\mathcal{M}_0(N)_{T^{(N)}}$ over $\mathbf{Z}[q, q^{-1}]$ is represented by*

$$\coprod_{dd'=N} \operatorname{Spec} \mathbf{Z}[\zeta_{d''}][q, q^{-1}][T]/(T^{d_1} - \zeta_{d''} q^{d'_1}).$$

Here, for d and d' satisfying $dd' = N$, d'' is the greatest common divisor of d and d', and $d_1 = d/d''$, $d'_1 = d'/d''$.

(2) *The functor $\mathcal{M}_1(N)_{T^{(N)}}$ over $\mathbf{Z}[q, q^{-1}]$ is represented by*

$$\coprod_{i=0}^{N-1} \operatorname{Spec} \mathbf{Z}[\zeta_{d'}][q, q^{-1}][T]/(T^{d} - \zeta_{d'} q^{i'}).$$

Here, for $0 \leq i < N$, d' is the greatest common divisor of N and i, and $d = N/d'$, $i' = i/d'$.

PROOF. (1) Let S be a scheme $\mathbf{Z}[q, q^{-1}]$. For a finite flat closed subgroup scheme $G \subset T_S^{(N)}$ over S and $i \in \mathbf{Z}$, let $G^i = G \cap T_S^{(N)i}$. G^0 is the kernel of $G \to T_S^{(N)} \to \mathbf{Z}/N\mathbf{Z}$ and is a closed subgroup scheme of $T_S^{(N)0} = \mathbf{G}_{m,s}$ that is finite flat over S.

Let d be a divisor of N, and let $d' = N/d$. Define the subfunctor $\mathcal{M}_0(N)^{(d)}_{T^{(N)}}$ of $\mathcal{M}_0(N)_{T^{(N)}}$ by associating the set

$$\mathcal{M}_0(N)^{(d)}_{T^{(N)}}(S) = \{G \in \mathcal{M}_0(N)_{T^{(N)}}(S) \mid G^0 \text{ is degree } d' \text{ over } S\}$$

to a scheme S over $\mathbf{Z}[q, q^{-1}]$. It suffices to show that the functor $\mathcal{M}_0(N)^{(d)}_{T^{(N)}}$ is represented by $\operatorname{Spec} \mathbf{Z}[\zeta_{d''}][q, q^{-1}][T]/(T^{d_1} - \zeta_{d''} q^{d'_1})$. By Proposition 8.14, G^0 has degree d' over S if and only if $G^0 = \mu_{d'}$. In this case, we also have $G = \coprod_{i=0}^{d-1} G^{d'i}$. We show the following lemma. ☐

LEMMA 8.27. *Let S be a scheme over $\mathbf{Z}[q, q^{-1}]$, and let $N = dd' \geq 1$ be an integer. Let d'' be the greatest common divisor of d and d', and let $d = d''d_1$.*

(1) *Let G be a closed subgroup scheme of $T_S^{(N)}$ that is finite flat of finite presentation over S of degree N and such that $G^0 = \mu_{d',S}$. Then, there exists a unique section $s : S \to T^{(N)d''}$ such that for each $0 \leq i < N$, the diagram*

$$\begin{tikzcd} G^{d'i} \arrow[r, "\subset"] \arrow[d] & T^{(N)d'i} \arrow[d, "{[d']}"] \\ S \arrow[r, "s^i"] & T^{(N)d'^2 i} \end{tikzcd} \tag{8.15}$$

is Cartesian. Moreover, s satisfies $s^d = 1$.

(2) *Conversely, suppose $s : S \to T^{(N)d'^2}$ is a section that satisfies $s^d = 1$. Define a closed subgroup scheme $G = \coprod_{i=0}^{d-1} G^{d'i}$ of $T_S^{(N)}$ by the condition that diagram (8.15) is Cartesian for each i. Then, G is a finite flat scheme of finite presentation over S of degree N, and $T_S^{(N)}$ is a closed subgroup scheme.*

(3) *Let G and s be as above. Then, G is a cyclic subgroup scheme if and only if s^{d_1} is a generator of $\mu_{d'',S}$.*

Proof. (1) Since $[d'] : T_S^{(N)d'} \to T_S^{(N)d''^2}$ is faithfully flat, a section $s : S \to T^{(N)d''^2}$ that satisfies the condition is unique once it exists. Thus, the assertion is flat local on S. Since $G^{d'}$ is a flat covering of S, we may assume $G^{d'}$ has a section $t : S \to G^{d'}$. For each i, the section $t : S \to G^{d'}$ defines the vertical isomorphisms in the diagram

$$\begin{tikzcd} \mu_{d'} \arrow[r] \arrow[d, "\times t^i"'] & \mathbf{G}_m \arrow[r, "{[d']}"] \arrow[d, "\times t^i"'] & \mathbf{G}_m \arrow[d, "\times t^{d'i}"] \\ G^{d'i} \arrow[r] & T_S^{(N)d'i} \arrow[r, "{[d']}"] & T_S^{(N)d'^2 i}. \end{tikzcd}$$

Thus, by letting $s = t^{d'}$, diagram (8.15) is Cartesian for each i. We have $s^d = t^N = 1$ by Proposition 8.14.

(2) Since $[d'] : \mathbf{G}_m \to \mathbf{G}_m$ is finite flat of degree d', G is a finite flat scheme of finite presentation of degree N. If $s^d = 1$, it is easy to see that G is a closed subgroup scheme of $T_S^{(N)}$.

(3) By Lemma 8.17, G is a cyclic subgroup scheme if and only if there exists a section P of $G^{d'}$ such that P^d is a generator of $\mu_{d'}$ flat locally on S, or equivalently, $G^{d'} \times_{[d]\searrow \mathbf{G}_m} \mu_{d'}^{\times} \to S$ has a section flat locally on S.

We have $G^{d'} \underset{[d]\searrow \mathbf{G}_m}{\times} \mu_{d'}^{\times} = S \underset{s\searrow T^{(N)d'^2}\swarrow [d']}{\times} T^{(N)d'} \underset{[d]\searrow \mathbf{G}_m}{\times} \mu_{d'}^{\times}$ by (8.15). By Lemma 8.19, all the vertical morphisms in the diagram

$$\begin{tikzcd}
T^{(N)d'} \arrow[r, "{[d]}"] \arrow[d, "{[d']}"'] & \mathbf{G}_m \arrow[d, "{[d_1']}"] & \mu_{d'}^{\times} \arrow[l] \arrow[d] \\
T^{(N)d'^2} \arrow[r, "{[d_1]}"'] & \mathbf{G}_m & \mu_{d''}^{\times} \arrow[l]
\end{tikzcd}$$

are faithfully flat. Thus, $G^{d'} \underset{[d]\searrow \mathbf{G}_m}{\times} \mu_{d'}^{\times} = S \underset{s\searrow T^{(N)d'^2}\swarrow [d']}{\times} T^{(N)d'} \underset{[d]\searrow \mathbf{G}_m}{\times} \mu_{d'}^{\times}$ is faithfully flat over the closed subscheme $S \underset{s\searrow T^{(N)d'^2}}{\times} T^{(N)d'^2} \underset{[d_1]\searrow \mathbf{G}_m}{\times} \mu_{d''}^{\times}$ of S. Therefore, the condition that $G^{d'} \underset{[d]\searrow \mathbf{G}_m}{\times} \mu_{d'}^{\times} \to S$ has a section flat locally on S is equivalent to the equality $S = S \underset{s\searrow T^{(N)d'^2}}{\times} T^{(N)d'^2} \underset{[d_1]\searrow \mathbf{G}_m}{\times} \mu_{d''}^{\times}$, and it is also equivalent to s^{d_1} being a generator of $\mu_{d'',S}$. □

Back to the proof of Proposition 8.26. By Lemma 8.27(1), we define an injection of functor $\mathcal{M}_0(N)^{(d)}_{T^{(N)}} \to T^{(N)d''^2}$ by associating s to G. Since $d = d''d_1$, if s^{d_1} is a generator of $\mu_{d'',S}$, then $s^d = 1$. Furthermore, by Lemma 8.27(2) and (3), the functor $\mathcal{M}_0(N)^{(d)}_{T^{(N)}}$ is represented by the closed subscheme $T^{(N)d''^2} \underset{[d_1]\searrow \mathbf{G}_m}{\times} \mu_{d''}^{\times}$ of $T^{(N)d''^2}$. By Lemma 8.19, $T^{(N)d''^2} \underset{[d_1]\searrow \mathbf{G}_m}{\times} \mu_{d''}^{\times}$ is the spectrum of

$$\begin{aligned}
&\mathbf{Z}[q,q^{-1}][T,T^{-1}] \otimes_{\mathbf{Z}[q,q^{-1}][T,T^{-1}]} \mathbf{Z}[\zeta_{d''}][q,q^{-1}] \\
&\qquad\qquad = \mathbf{Z}[\zeta_{d''}][q,q^{-1}][T]/(T^{d_1} - \zeta_{d''} q^{d_1'}).
\end{aligned}$$

Here, the tensor product is taken with respect to the homomorphism sending T to $T^{d_1}/q^{d_1 d''^2/N} = T^{d_1}/q^{d_1'}$ and the homomorphism sending T to $\zeta_{d''}$.

(2) Suppose $0 \leq i < N$. Let $d \mid N$ be the order of $i \in \mathbf{Z}/N\mathbf{Z}$, and let $dd' = N$. By Lemma 8.17, a section P of $T^{(N)i}$ over S has exact order N if and only if P^d is a generator of $\mu_{d'}$. Thus, we have

$$\mathcal{M}_1(N)_{T^{(N)}} = \coprod_{i=0}^{N-1} T^{(N)i} \underset{[d]\searrow \mathbf{G}_m}{\times} \mu_{d'}^{\times}. \tag{8.16}$$

$T^{(N)i} \underset{[d]\searrow \mathbf{G}_m}{\times} \mu_{d'}^{\times}$ is the spectrum of

$$\begin{aligned}\mathbf{Z}[q,q^{-1}][T,T^{-1}] \otimes_{\mathbf{Z}[q,q^{-1}][T,T^{-1}]} \mathbf{Z}[\zeta_{d'}][q,q^{-1}]& \\ = \mathbf{Z}[\zeta_{d'}][q,q^{-1}][T]/(T^d - \zeta_{d'}q^{i'}).&\end{aligned}$$

Here, the tensor product is taken with respect to the homomorphism sending T to $T^d/q^{di/N}$ and the homomorphism sending T to $\zeta_{d''}$.

8.4. Modular curves over Z

DEFINITION 8.28. Let $N \geq 1$ be an integer.

(1) Define a functor $\mathcal{M}_0(N)$ over **Z** by associating to a scheme T the set

$$\mathcal{M}_0(N)(T) = \left\{ \begin{array}{l} \text{isomorphism classes of pairs } (E, C), \\ \text{where } E \text{ is an elliptic curve over } T, \\ \text{and } C \text{ is its cyclic subgroup scheme of} \\ \text{order } N \end{array} \right\}. \tag{8.17}$$

(2) Define a functor $\mathcal{M}_1(N)$ over **Z** by associating to a scheme T the set

$$\mathcal{M}_1(N)(T) = \left\{ \begin{array}{l} \text{isomorphism classes of pairs } (E, P), \\ \text{where } E \text{ is an elliptic curve over } T, \\ \text{and } P \text{ is its section of exact order } N \end{array} \right\}. \tag{8.18}$$

By associating to an isomorphism class of (E, P) the isomorphism class of $(E, \langle P\rangle)$, we define a morphism of functors

$$\mathcal{M}_1(N) \longrightarrow \mathcal{M}_0(N). \tag{8.19}$$

LEMMA 8.29. *Let $N = 4$. The restriction of the functor $\mathcal{M}_1(4)$ to $\mathbf{Z}[\frac{1}{4}]$ is represented by*

$$Y_1(4)_{\mathbf{Z}[\frac{1}{4}]} = \operatorname{Spec} \mathbf{Z}\left[\frac{1}{4}, d, \frac{1}{d(d-4)}\right]. \tag{8.20}$$

The universal elliptic curve E and the universal section P of order 4 are given by

$$E : dy^2 = x^3 + (d-2)x^2 + x, \quad P = (1,1). \tag{8.21}$$

PROOF. Let S be a scheme over $\mathbf{Z}[\frac{1}{4}]$, let $f : E \to S$ be an elliptic curve over S, and let P be a section of exact order 4. Let O be the 0-section, and let $Q = 2P$ and $R = 3P$. Let x be the inverse image of 1 by the isomorphism $f_*\mathcal{O}(2[O] - 2[Q]) \to \mathcal{O}_P$, and let y be the inverse image of 1 by the isomorphism $f_*\mathcal{O}(3[O]-(2[P]+[Q])) \to \mathcal{O}_P$. Define the immersion $E \to \mathbf{P}^2_S$ by the basis x, y, 1 of $f_*\mathcal{O}(3[O])$. Then x and

y satisfy an equation of the form $y^2 + a_1xy + a_3y = a_0x^3 + a_2x^2 + a_4x + a_6$ ($a_i \in \mathcal{O}_S$), which defines E. Since the three points O, P, R are collinear, the coordinates of O, P, Q, R are $(0 : 1 : 0)$, $(1 : 0 : 1)$, $(0 : 0 : 1)$, and $(1 : 1 : 1)$, respectively.

In the inhomogeneous coordinates, E is tangent to the line $x = 0$ at $Q = (0, 0)$, intersects with the line $y = 0$ at Q, is tangent to it at $P = (1, 0)$, and passes through $R = (1, 1)$. Thus, we have $a_6 = a_3 = 0$, $a_0x^3 + a_2x^2 + a_4x + a_6 = a_0x(x - 1)^2$, and $a_1 = -1$. Hence, the elliptic curve E is defined by the equation $y^2 - xy = a_0x(x - 1)^2$, where $a_0 \in \mathcal{O}_S^\times$. Let $a_0 = d/4$, and substitute $x - 2y$ by y. Then, the equation $4d(y^2 - xy) = x(x - 1)^2$ becomes $dy^2 = dx^2 + x(x - 1)^2$. The condition that the right-hand side has a triple root is $d = 0, 4$. ☐

If $N = 1$, we have $\mathcal{M}_0(1) = \mathcal{M}_1(1)$. We will denote them simply by $\mathcal{M}$. For a scheme T, we have

$$\mathcal{M}(T) = \{\text{isomorphism classes of elliptic curves } E \text{ over } T\}. \tag{8.22}$$

Associating E to the isomorphism class of (E, C) or that of (E, P), we obtain morphisms of functors

$$\mathcal{M}_0(N) \longrightarrow \mathcal{M} \text{ and } \mathcal{M}_1(N) \longrightarrow \mathcal{M}. \tag{8.23}$$

The functor $\mathcal{M}$ defined in Example 2.4 of Chapter 2 is $\mathcal{M}_{\mathbf{Q}}$; i.e., the restriction to $\mathbf{Q}$ of the functor $\mathcal{M}$ just defined. In Example 2.6, we defined the morphism of functors $j : \mathcal{M}_{\mathbf{Q}} \to \mathbf{A}^1_{\mathbf{Q}}$ over $\mathbf{Q}$. This is extended naturally to a morphism of functors $j : \mathcal{M} \to \mathbf{A}^1_{\mathbf{Z}}$ over $\mathbf{Z}$.

LEMMA 8.30. (1) *There exists a unique morphism of functors $j : \mathcal{M} \to \mathbf{A}^1_{\mathbf{Z}}$ over $\mathbf{Z}$ that extends the morphism of functors $j : \mathcal{M}_{\mathbf{Q}} \to \mathbf{A}^1_{\mathbf{Q}}$ over $\mathbf{Q}$.*

(2) *For any algebraically closed field k, the mapping $j : \mathcal{M}(k) \to \mathbf{A}^1_{\mathbf{Z}}(k) = k$ is a bijection.*

QUESTION. Prove Lemma 8.30. (*Hint*: To show the uniqueness, it suffices to consider the elliptic curve E over

$$A = \mathbf{Z}[a_1, a_2, a_3, a_4, a_6]\left[\frac{1}{\Delta}\right]$$

defined by the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. To show the existence, verify $j(E) \in A$, and it is invariant under the change of coordinates.)

EXAMPLE 8.31. The j-invariant of the elliptic curve $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ over $\mathbf{Z}[\frac{1}{2},\alpha,\beta,\gamma][\Delta^{-1}]$, where $\Delta = ((\alpha-\beta)(\beta-\gamma)(\gamma-\alpha))^2$, is given by

$$2^8 \cdot \frac{(\alpha^2+\beta^2+\gamma^2-\alpha\beta-\beta\gamma-\gamma\alpha)^3}{\Delta}. \tag{8.24}$$

Thus the j-invariant of the elliptic curve $y^2 = x(x^2+ax+b)$ over $\mathbf{Z}[\frac{1}{2},a,b][b^{-1},(a^2-4b)^{-1}]$ is given by

$$2^8 \cdot \frac{(a^2-3b)^3}{b^2(a^2-4b)}. \tag{8.25}$$

The j-invariant of the universal elliptic curve $dy^2 = x(x^2+(d-2)x+1)$ over $Y_1(4)_{\mathbf{Z}[\frac{1}{2}]}$ is given by

$$2^8 \cdot \frac{(d^2-4d+1)^3}{d(d-4)}. \tag{8.26}$$

Suppose $a \in (\mathbf{Z}/N\mathbf{Z})^\times$. If P is a section of exact order N, then aP also has exact order N. Thus, by associating to the isomorphism of (E,P) the isomorphism class of (E,aP), we obtain an isomorphism of functors

$$\langle a\rangle : \mathcal{M}_1(N) \longrightarrow \mathcal{M}_1(N). \tag{8.27}$$

This is called the *diamond operator*. The diamond operator $\langle a\rangle : \mathcal{M}_1(N) \to \mathcal{M}_1(N)$ is an automorphism over $\mathcal{M}_0(N)$. Since (E,P) is isomorphic to $(E,-P)$, we have $\langle -1\rangle = 1$.

If $N = N'N''$ with $(N',N'')=1$, we have an identification

$$\mathcal{M}_0(N)(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E,C',C''), \\ \text{where } E \text{ is an elliptic curve over } T,\ C' \text{ is} \\ \text{its cyclic subgroup scheme of order } N', \\ \text{and } C'' \text{ is its cyclic subgroup scheme of} \\ \text{order } N'' \end{array} \right\}.$$

Similarly,

$$\mathcal{M}_1(N)(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E,P',P''), \\ \text{where } E \text{ is an elliptic curve over } T,\ P' \text{ is} \\ \text{its section of exact order } N', \text{ and } P'' \text{ is its} \\ \text{section of exact order } N'' \end{array} \right\}.$$

Associating to the isomorphism class of triples (E,C',C'') the isomorphism class of triples $(E/C', E[N']/C', (C''+C')/C')$, we obtain a morphism of functors

$$w_{N'} : \mathcal{M}_0(N) \longrightarrow \mathcal{M}_0(N), \tag{8.28}$$

called the *Atkin–Lehner involution*. It is easy to see $w_{N'}^2$ is the identity.

Let $N \geq 1$ be an integer, and let p be a prime number. We denote by $\mathcal{M}_0(N)_{\mathbf{F}_p}$ the restriction of the functor $\mathcal{M}_0(N)$ to schemes over $\mathbf{F}_p$. To the isomorphism class of a pair (E, C), we associate the isomorphism class of $(E^{(p)}, C^{(p)})$ to obtain a morphism of functors $F : \mathcal{M}_0(N)_{\mathbf{F}_p} \to \mathcal{M}_0(N)_{\mathbf{F}_p}$. We call it the *Frobenius morphism.* Define a subfunctor $\mathcal{M}_0(N)_{\mathbf{F}_p}^{\mathrm{ss}}$ of $\mathcal{M}_0(N)_{\mathbf{F}_p}$ by associating to a scheme T over $\mathbf{F}_p$ the set

$$\mathcal{M}_0(N)_{\mathbf{F}_p}^{\mathrm{ss}}(T) = \left\{ \begin{array}{l} \text{isomorphism classes of pairs } (E, C), \\ \text{where } E \text{ is a supersingular elliptic} \\ \text{curve over } T, \text{ and } C \text{ is its cyclic sub-} \\ \text{group scheme of order } N \end{array} \right\}. \tag{8.29}$$

Define the restriction of functor $\mathcal{M}_1(N)_{\mathbf{F}_p}$ and the Frobenius morphism $\mathcal{M}_1(N)_{\mathbf{F}_p} \to \mathcal{M}_1(N)_{\mathbf{F}_p}$ similarly.

Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p. Let $N = Mp$. Define a morphism of functors over $\mathbf{F}_p$ $j_0 : \mathcal{M}_0(M)_{\mathbf{F}_p} \to \mathcal{M}_0(N)_{\mathbf{F}_p}$ by associating to the isomorphism class of a pair (E, C) the isomorphism class of $(E, C, \operatorname{Ker} F)$. Also, define $j_1 : \mathcal{M}_0(M)_{\mathbf{F}_p} \to \mathcal{M}_0(N)_{\mathbf{F}_p}$ by associating to the isomorphism class of a pair (E, C) the isomorphism class of $(E^{(p)}, C^{(p)}, \operatorname{Ker} V)$.

In this chapter we show the following theorem.

THEOREM 8.32. *Let $N \geq 1$ be an integer.*

(1) *There exists a coarse moduli scheme $Y_0(N)_{\mathbf{Z}}$ of $\mathcal{M}_0(N)$ over $\mathbf{Z}$. $Y_0(N)_{\mathbf{Z}}$ is a normal connected affine curve over $\mathbf{Z}$.*

(2) *The morphism*

$$Y_0(N)_{\mathbf{Z}} \longrightarrow Y(1)_{\mathbf{Z}} \tag{8.30}$$

induced by the morphism of functors $\mathcal{M}_0(N) \to \mathcal{M}$ (8.23) is finite flat of degree $\psi(N)$.

(3) *$Y_0(N)_{\mathbf{Z}}$ is smooth over $\mathbf{Z}[\frac{1}{N}]$. For a prime number $p \nmid N$, $Y_0(N)_{\mathbf{F}_p} = Y_0(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p$ is the coarse moduli scheme of the restriction $\mathcal{M}_0(N)_{\mathbf{F}_p}$.*

(4) *Let p be a prime number, and assume $N = Mp$ for an integer M prime to p. Then, $Y_0(N)_{\mathbf{Z}}$ is weakly semistable at p. The morphisms $j_0, j_1 : \mathcal{M}_0(M)_{\mathbf{F}_p} \to \mathcal{M}_0(N)_{\mathbf{F}_p}$ over $\mathbf{F}_p$ induce closed immersions $j_0, j_1 : Y_0(M)_{\mathbf{F}_p} \to Y_0(N)_{\mathbf{Z}}$. The fiber $Y_0(N)_{\mathbf{F}_p}$ is the union of the image C_0 of j_0 and the image C_1 of j_1. The intersection of $C_0 = Y_0(M)_{\mathbf{F}_p}$ and C_1 is the*

coarse moduli $Y_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$ *of* $\mathcal{M}_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$. *The index* e_x *of the ordinary double point* $x = [(E, C)] \in Y_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$ *is the order of* $\mathrm{Aut}(E_{\overline{\mathbf{F}}_p}, C_{\overline{\mathbf{F}}_p})/\{\pm 1\}$.

The fiber $Y_0(N)_{\mathbf{Q}} = Y_0(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q}$ of $Y_0(N)_{\mathbf{Z}}$ at the generic point is the modular curve $Y_0(N)_{\mathbf{Q}}$ over $\mathbf{Q}$ that we constructed in Theorem 2.10.

EXAMPLE 8.33. Replacing y by $1+2y$, the defining equation (1.3) $y^2 = 4x^3 - 4x^2 - 40x - 79$ of $X_0(11)_{\mathbf{Q}}$ becomes

$$y^2 + y = x^3 - x^2 - 10x - 20. \tag{8.31}$$

The homogeneous equation of (8.31) defines an elliptic curve over $\mathbf{Z}[\frac{1}{11}]$, and the fiber of $\mathbf{F}_{11}$ is the Néron 1-gon. If we let $s = \frac{y-60}{x-16}$, (8.31) becomes $s^2(x-16) + 121s = x^2 + 15x + 230$. The morphism

$$\begin{aligned}\operatorname{Spec} \mathbf{Z}[x, s]/(s^2(x-16) + 121s - (x^2 + 15x + 230))\\ \to \operatorname{Spec} \mathbf{Z}[x, y]/(y^2 + y - (x^3 - x^2 - 10x - 20))\end{aligned}$$

is an open immersion over $\mathbf{Z}[\frac{1}{11}]$. Through this immersion, we identify

$$Y_0(11)_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[x, s]/(s^2(x-16) + 121s - (x^2 + 15x + 230)).$$

We have $Y_0(11)_{\mathbf{F}_{11}} = \operatorname{Spec} \mathbf{F}_{11}[x, s]/((s^2 - (x-2))(x-5))$, and the curve $Y_0(11)_{\mathbf{Z}}$ over $\mathbf{Z}$ is weakly semistable at $p = 11$. It has two ordinary double points, $(x, s) = (5, 5)$ and $(5, 6)$. Their indices are 2 and 3, respectively.

THEOREM 8.34. *Let* $N \geq 1$ *be an integer.*

(1) *There exists a coarse moduli scheme* $Y_1(N)_{\mathbf{Z}}$ *of* $\mathcal{M}_1(N)$ *over* $\mathbf{Z}$. *If* $N \geq 4$, $Y_1(N)_{\mathbf{Z}[\frac{1}{N}]}$ *is a fine moduli scheme.* $Y_1(N)_{\mathbf{Z}}$ *is a normal connected affine curve over* $\mathbf{Z}$.

$Y_1(N)_{\overline{\mathbf{Q}}} = Y_1(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \overline{\mathbf{Q}}$ *is a smooth connected affine curve over* $\overline{\mathbf{Q}}$.

(2) *The morphism*

$$Y_1(N)_{\mathbf{Z}} \longrightarrow Y(1)_{\mathbf{Z}} \tag{8.32}$$

induced by the morphism of functors $\mathcal{M}_1(N) \to \mathcal{M}$ (8.23) *is finite flat of degree* $\psi(N)\phi(N)/2$ *if* $N \geq 3$, *and of degree* 3 *if* $N = 2$.

(3) $Y_1(N)_{\mathbf{Z}}$ *is smooth over* $\mathbf{Z}[\frac{1}{N}]$. *For a prime number* $p \nmid N$, $Y_1(N)_{\mathbf{F}_p} = Y_1(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p$ *is a coarse moduli scheme of the restriction* $\mathcal{M}_1(N)_{\mathbf{F}_p}$.

REMARK. The modular curves $Y_0(N)_{\mathbf{Z}}$ and $Y_1(N)_{\mathbf{Z}}$ are the integral closures of $Y_0(N)_{\mathbf{Z}[\frac{1}{N}]}$ and $Y_1(N)_{\mathbf{Z}[\frac{1}{N}]}$, respectively, by Theorems 8.32 and 8.34. However, if we defined $Y_0(N)_{\mathbf{Z}}$ and $Y_1(N)_{\mathbf{Z}}$ as the integral closures, their detailed structures could not be studied any further. The definition using the Drinfeld level structures is the only way for us to study their detailed structures, which we will do starting from §8.6.

8.5. Modular curve $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$

In order to prove Theorems 8.32 and 8.34, we define auxiliary functors.

DEFINITION 8.35. Let $N \geq 1$ be an integer, and let $r \geq 1$ be an integer relatively prime to N.

(1) Define the functor $\mathcal{M}_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ by associating to a scheme T over $\mathbf{Z}[\frac{1}{r}]$ the set

(8.33)
$$\mathcal{M}_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E,C,\alpha), \\ \text{where } E \text{ is an elliptic curve over } T,\ C \text{ is its} \\ \text{cyclic subgroup scheme of order } N, \text{ and} \\ \alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r] \text{ is an isomorphism} \end{array} \right\}.$$

(2) Define the functor $\mathcal{M}_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ by associating to a scheme T over $\mathbf{Z}[\frac{1}{r}]$ the set

(8.34)
$$\mathcal{M}_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E,P,\alpha), \\ \text{where } E \text{ is an elliptic curve over } T, \\ P \text{ is a section of exact order } N, \text{ and} \\ \alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r] \text{ is an isomorphism} \end{array} \right\}.$$

The natural action of $\mathrm{GL}(2,\mathbf{Z}/r\mathbf{Z})$ on $(\mathbf{Z}/r\mathbf{Z})^2$ induces actions of $\mathrm{GL}(2,\mathbf{Z}/r\mathbf{Z})$ on $\mathcal{M}_{0,*}(1,r)_{\mathbf{Z}[\frac{1}{r}]}$ and on $\mathcal{M}_{1,*}(1,r)_{\mathbf{Z}[\frac{1}{r}]}$. If $N=1$, we have $\mathcal{M}_{0,*}(1,r)_{\mathbf{Z}[\frac{1}{r}]} = \mathcal{M}_{1,*}(1,r)_{\mathbf{Z}[\frac{1}{r}]}$, which we denote simply by $\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{r}]}$.

EXAMPLE 8.36. Let $r=3$. The functor $\mathcal{M}(3)_{\mathbf{Z}[\frac{1}{3}]}$ is represented by

(8.35)
$$Y(3)_{\mathbf{Z}[\frac{1}{3}]} = \operatorname{Spec} \mathbf{Z}\left[\frac{1}{3}, \zeta_3, \mu, \frac{1}{\mu^3-1}\right].$$

The universal curve (E, O) and the universal base α are given respectively by

$$\begin{aligned} E &: X^3+Y^3+Z^3-3\mu XYZ=0, \quad O:(0,1,-1), \\ \alpha &: (1,0)\mapsto(0,\zeta_3,-1),\ (0,1)\mapsto(1,0,-1). \end{aligned} \tag{8.36}$$

QUESTION. Verify Example 8.36. (*Hint*: Use the proof of Theorem 2.21 for the case $N = 3$.)

Let $r, s \geq 1$ be integers. Let H be the kernel

$$\operatorname{Ker}\bigl(\mathrm{GL}_2(\mathbf{Z}/rs\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})\bigr).$$

Define a morphism of functors over $\mathbf{Z}[\frac{1}{rs}]$

$$\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{rs}]} \longrightarrow [\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H] \tag{8.37}$$

as follows. Let S be a scheme over $\mathbf{Z}[\frac{1}{rs}]$, let E be an elliptic curve over S, and let $\alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r]$ be an isomorphism. Define a functor $\mathcal{I}som_\alpha((\mathbf{Z}/rs\mathbf{Z})^2, E[rs])$ over S by associating to a scheme T over S the set

$$\begin{aligned} &\mathcal{I}som_\alpha\bigl((\mathbf{Z}/rs\mathbf{Z})^2, E[rs]\bigr)(T) \\ &\qquad = \{\text{isomorphism } \beta : (\mathbf{Z}/rs\mathbf{Z})^2 \to E_T[rs] \mid \beta \text{ induces } \alpha\}. \end{aligned}$$

The functor $\mathcal{I}som_\alpha\bigl((\mathbf{Z}/rs\mathbf{Z})^2, E[rs]\bigr)$ is represented by an H-torsor P over S. The element of $\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}(P)$ defined by the pair (E_P, β) of the pullback E_P of E to P, and the universal isomorphism β over P is compatible with the action of H. Thus, it defines an element of $[\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H](S)$. We thus have a morphism $\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{rs}]} \to [\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H]$.

Similarly, for relatively prime integers $N, r \geq 1$, we define morphisms of functors over $\mathbf{Z}[\frac{1}{r}]$

$$\begin{aligned} \mathcal{M}_0(N)_{\mathbf{Z}[\frac{1}{r}]} &\longrightarrow [\mathcal{M}_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}/\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})], \\ \mathcal{M}_1(N)_{\mathbf{Z}[\frac{1}{r}]} &\longrightarrow [\mathcal{M}_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}/\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})]. \end{aligned} \tag{8.38}$$

LEMMA 8.37. *Let $r \geq 3$ be an integer. The functor $\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ is represented by a smooth affine connected curve $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$.*

The field of constants of $Y(r)_{\mathbf{Q}} = Y(r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ is $\mathbf{Q}(\zeta_r)$.

$Y(r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ is the modular curve $Y(r)$ constructed in Theorem 2.21. Lemma 8.37 is proved in the same way as in §2.4.

PROOF. If $r = 3$, it is given by Example 8.36. If $r = 4$, take (E, P) where E is the universal elliptic curve over $Y_1(4)_{\mathbf{Z}[\frac{1}{4}]}$ and P is the universal element of order 4. Let Q be the diagonal section of E over $E[4]$. Let $Y(4)_{\mathbf{Z}[\frac{1}{4}]}$ be the closed and open subscheme of $E[4]$ defined by the condition that (P, Q) gives a basis of $E[4]$. Then $\mathcal{M}(4)_{\mathbf{Z}[\frac{1}{4}]}$ is represented by $Y(4)_{\mathbf{Z}[\frac{1}{4}]}$. If r is a multiple of 3, $\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{r}]}$ is represented by the finite étale scheme $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ over $Y(3)_{\mathbf{Z}[\frac{1}{r}]}$. The case where r is a multiple of 4 is similar.

We show the general case. To do so, we first show the following lemma.

LEMMA 8.38. *Let S be a scheme, let $f : E \to S$ be an elliptic curve, and let g be an automorphism of E over S.*

(1) *Let $r \geq 3$ be an integer, and let S be a scheme over $\mathbf{Z}[\frac{1}{r}]$. If the restriction $g|_{E[r]}$ is the identity morphism, then so is g.*
(2) *Let $N \geq 4$ be an integer, and let S be a scheme over $\mathbf{Z}[\frac{1}{N}]$. Let C be a cyclic subgroup scheme of E of order N. If the restriction $g|_C$ is the identity morphism, then so is g.*

PROOF. The invertible sheaf $\mathcal{L} = \mathcal{O}(3[O])$ on E defines a closed immersion $E \to \mathbf{P}(f_*\mathcal{L})$.

(1) Let $D \geq 0$ be the Cartier divisor defined by $D = [E[r]] - [O]$. Since r is invertible on S, we have $D \cap O = \varnothing$, and $\mathcal{L}|_D = \mathcal{O}|_D$. Moreover, since $r \geq 3$, we have $\deg D = r^2 - 1 > 3$, and $f_*\mathcal{L} \to \mathcal{L}|_D$ is injective. Thus, if $g|_{E[r]}$ is the identity, the action of g on $f_*\mathcal{L} \subset \mathcal{L}|_D = \mathcal{O}_D$ is trivial, and so is the action on $\mathbf{P}(f_*\mathcal{L})$. Hence, the action of g on E is also trivial.

(2) Let $D = C - [O]$. If $N \geq 5$, we have $\deg D = N - 1 > 3$. Then, the proof goes similarly to (1). If $N = 4$, let $P \in C$ be the section of exact order 2. Then, by Example D.4, we have $\mathcal{L}(-D) \simeq \mathcal{O}([P] - [O])$ locally on S. Thus $f_*\mathcal{L} \to \mathcal{L}|_D$ is injective, and the rest is similar to the proof of (1). □

COROLLARY 8.39. (1) *Let $s \geq 1$ be an integer, and let $H = \mathrm{Ker}\big(\mathrm{GL}_2(\mathbf{Z}/rs\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})\big)$. If $r \geq 3$, the morphism of functors $\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{rs}]} \to [\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H]$ (8.37) over $\mathbf{Z}[\frac{1}{rs}]$ is an isomorphism.*

(2) *Let $N \geq 4$ be an integer relatively prime to r. The morphism of functors $\mathcal{M}_1(N)_{\mathbf{Z}[\frac{1}{Nr}]} \to [\mathcal{M}_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{Nr}]}/\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})]$ (8.38) over $\mathbf{Z}[\frac{1}{Nr}]$ is an isomorphism.*

PROOF. (1) We construct the inverse morphism. Let S be a scheme over $\mathbf{Z}[\frac{1}{rs}]$. Let P be an H-torsor over S, and let $(E,\beta) \in \mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}(P)$ be an H-invariant pair of an elliptic curve over P and an isomorphism $\beta : (\mathbf{Z}/rs\mathbf{Z})^2 \to E[rs]$. Let $\alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r]$ be the isomorphism induced by β. Let $g \in H$. Then, by the assumption $r \geq 3$ and Lemma 8.38(1), there exists a unique isomorphism $g^*(E,\beta) = P \underset{g \searrow P}{\times} (E,\beta) \to (E, \beta \circ g)$ over P. Thus, the action of H on P extends uniquely to a free action on E, the quotient $E_S = E/H$ is an elliptic curve over S, and the natural morphism $E_S \times_S P \to E$ is an isomorphism. Moreover, the isomorphism $\alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r]$ is the pullback of an isomorphism $\alpha_S : (\mathbf{Z}/r\mathbf{Z})^2 \to E_S[r]$. Sending (E,β) to (E_S, α_S), we obtain the inverse morphism $\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{rs}]} \to [\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H]$.

(2) We construct the inverse morphism. Let S be a scheme over $\mathbf{Z}[\frac{1}{Nr}]$, and let Q be a $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$-torsor over S. Let

$$(E, P, \alpha) \in \mathcal{M}_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{Nr}]}(Q)$$

be a $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$-invariant triple of an elliptic curve E over Q, a section P of exact order N, and an isomorphism $\alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r]$. The section P defines an isomorphism $\mathbf{Z}/N\mathbf{Z} \to \langle P \rangle \subset E$. Suppose $g \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. Then, by the assumption $N \geq 4$ and Lemma 8.38(2), there exists a unique isomorphism $g^*(E,P) \to (E,P)$ over Q. The rest is similar to the proof of (1). $\square$

We show Lemma 8.37 when r is general. Suppose $s = 3$ or 4. The functor $\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}$ is represented by $Y(rs)_{\mathbf{Z}[\frac{1}{rs}]}$. By Lemma 8.38(1), the natural action of $H = \mathrm{Ker}\big(\mathrm{GL}_2(\mathbf{Z}/rs\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})\big)$ on $Y(rs)_{\mathbf{Z}[\frac{1}{rs}]}$ is free. Thus, by Lemmas A.31 and A.33, the natural morphism $Y(rs)_{\mathbf{Z}[\frac{1}{rs}]} \to Y(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H$ is finite and étale, and the quotient $Y(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H$ represents the functor $[\mathcal{M}(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H]$ over $\mathbf{Z}[\frac{1}{rs}]$. By Corollary 8.39(1), the quotient $Y(r)_{\mathbf{Z}[\frac{1}{rs}]} = Y(rs)_{\mathbf{Z}[\frac{1}{rs}]}/H$ represents the functor $\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{rs}]}$. Moreover, $Y(r)_{\mathbf{Z}[\frac{1}{rs}]}$ is a smooth affine curve over $\mathbf{Z}[\frac{1}{rs}]$. $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is obtained by gluing $Y(r)_{\mathbf{Z}[\frac{1}{3r}]}$ and $Y(r)_{\mathbf{Z}[\frac{1}{4r}]}$ on $Y(r)_{\mathbf{Z}[\frac{1}{6r}]}$.

Let $(\ ,\ )_{E[r]} : E[r] \times E[r] \to \mu_r$ be the Weil pairing. Associating to the pair (E,α) the root of unity $(\alpha(1,0), \alpha(0,1))_{E[r]}$, we obtain $Y(r)_{\mathbf{Z}[\frac{1}{r}]} \to \mathbf{Z}[\frac{1}{r}, \zeta_r]$. To show that the field of constants of $Y(r)_{\mathbf{Q}} = Y(r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ is $\mathbf{Q}(\zeta_r)$, it suffices to show that the Riemann surface

$Y(r)^{\mathrm{an}}$ defined by $Y(r)_{\mathbf{C}} = Y(r)_{\mathbf{Q}} \otimes_{\mathbf{Q}(\zeta_r)} \mathbf{C}$ is connected. Let $\Gamma(r)$ be the subgroup of $\mathrm{SL}_2(\mathbf{Z})$ defined by

$$\Gamma(r) = \mathrm{Ker}\big(\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/r\mathbf{Z})\big), \tag{8.39}$$

and consider the natural action of $\Gamma(r)$ on the upper half-plane $H = \{\tau \in \mathbf{C} \mid \mathrm{Im}\,\tau > 0\}$. As in Corollary 2.66, we obtain an isomorphism of Riemann surfaces

$$\Gamma(r)\backslash H \longrightarrow Y(r)^{\mathrm{an}}. \tag{8.40}$$

Thus $Y(r)^{\mathrm{an}}$ is connected and $Y(r)_{\mathbf{Q}(\zeta_r)}$ is a smooth connected affine curve over $\mathbf{Q}(\zeta_r)$. □

COROLLARY 8.40. (1) *There exists a coarse moduli scheme* $Y(1)_{\mathbf{Z}}$ *of the functor* $\mathcal{M}$.

(2) *The morphism of functors* $\mathcal{M} \to \mathbf{A}^1_{\mathbf{Z}}$ *defined by the* j*-invariant induces an isomorphism*

$$j : Y(1)_{\mathbf{Z}} \longrightarrow \mathbf{A}^1_{\mathbf{Z}}. \tag{8.41}$$

(3) *Let* $r \geq 3$ *be an integer. The restriction of the natural morphism* $j : Y(r)_{\mathbf{Z}[\frac{1}{r}]} \to Y(1)_{\mathbf{Z}} = \mathbf{A}^1_{\mathbf{Z}}$ *to* $U = \mathrm{Spec}\,\mathbf{Z}\big[j, \frac{1}{j(j-12^3)}\big] \subset \mathbf{A}^1_{\mathbf{Z}}$

$$Y(r)_{\mathbf{Z}[\frac{1}{r}]} \times_{\mathbf{A}^1_{\mathbf{Z}}} U \longrightarrow U$$

is a $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/\{\pm 1\}$*-torsor.*

PROOF. (1) As in the proof of Lemmas 2.27 and 8.37, the coarse moduli scheme $Y(1)_{\mathbf{Z}}$ of $\mathcal{M}$ is obtained by gluing the quotient of $Y(3)_{\mathbf{Z}[\frac{1}{3}]}$ by $\mathrm{GL}_2(\mathbf{Z}/3\mathbf{Z})$ and the quotient of $Y(4)_{\mathbf{Z}[\frac{1}{4}]}$ by $\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z})$.

(2) By the construction in (1), $Y(1)_{\mathbf{Z}}$ is a normal affine curve over $\mathbf{Z}$. Since $j : Y(1)_{\mathbf{Z}} \to \mathbf{A}^1_{\mathbf{Z}}$ is an isomorphism over $\mathbf{Q}$, it is a birational morphism. Moreover, by Lemma 8.30(2), the morphism of normal schemes $j : Y(1)_{\mathbf{Z}} \to \mathbf{A}^1_{\mathbf{Z}}$ induces a bijection on each geometric fiber, and thus it is an isomorphism.

(3) The natural action of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ on $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is an action as an automorphism over $Y(1)_{\mathbf{Z}}$. Since the multiplication-by-(-1) morphism is an automorphism of the universal elliptic curve, the action of $-1 \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ on $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is trivial. Since $Y(r)_{\mathbf{Z}[\frac{1}{r}]} \to Y(1)_{\mathbf{Z}[\frac{1}{r}]}$ is a finite morphism of regular schemes, it suffices to show, by Lemma A.34, that each geometric fiber over $U = \mathrm{Spec}\,\mathbf{Z}[\frac{1}{r}][j, \frac{1}{j(j-12^3)}]$ is a $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/\{\pm 1\}$-torsor. Let k be an algebraically closed field with $r \in k^\times$, and let E be an elliptic curve over k with $j(E) \neq 0, 12^3$. Since $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is a fine moduli scheme, the fiber of the morphism

$Y(r)_{\mathbf{Z}[\frac{1}{r}]} \to Y(1)$ at $j(E) \in \mathbf{A}^1(k) = Y(1)_{\mathbf{Z}[\frac{1}{r}]}(k)$ is identified with $\mathcal{I}som((\mathbf{Z}/r\mathbf{Z})^2, E[r])/\{\pm 1\}$. This is a $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/\{\pm 1\}$-torsor since we have $\mathrm{Aut}(E) = \{\pm 1\}$ by Lemma 8.41 below. □

LEMMA 8.41. *Let k be an algebraically closed field of characteristic $p \geq 0$, and let E be an elliptic curve over k.*

(1) *The automorphism group $\mathrm{Aut}(E)$ is finite, and the order of $g \in \mathrm{Aut}(E)$ is either a divisor of 4 or a divisor of 6.*
(2) *If $j(E) \neq 0, 12^3$, then $\mathrm{Aut}(E) = \{\pm 1\}$.*
(3) *If $p \neq 2, 3$ and $j(E) = 0$, then $\mathrm{Aut}(E) = \mu_6$.*
(4) *If $p \neq 2, 3$ and $j(E) = 12^3$, then $\mathrm{Aut}(E) = \mu_4$.*
(5) *If $p = 3$ and $j(E) = 0 = 12^3$, then $\sharp\,\mathrm{Aut}(E) = 12$, and $1 \to \{\pm 1\} \to \mathrm{Aut}(E) \to \mathrm{Aut}(E[2]) \to 1$ is an exact sequence.*
(6) *If $p = 2$ and $j(E) = 0 = 12^3$, then $\sharp\,\mathrm{Aut}(E) = 24$, and the natural mapping $\mathrm{Aut}(E) \to \mathrm{Aut}(E[3], (\ ,\ )_3) \simeq \mathrm{SL}_2(\mathbf{F}_3)$ is an isomorphism.*

PROOF. (1) Let $r \geq 3$ be an integer invertible in k. Since $\mathrm{Aut}(E) \to \mathrm{Aut}(E[r])$ is injective by Lemma 8.38(1), $\mathrm{Aut}(E)$ is a finite group. If $g \in \mathrm{Aut}(E)$, then the order of g is finite. The characteristic polynomial $\det(T - g) \in \mathbf{Z}[T]$ is of degree 2, and its leading coefficient and constant term are both 1. Thus, the coefficient of T must be one of $0, \pm 1, \pm 2$, and the order of g is one of $1, 2, 3, 4$, and 6.

(2) (3) (4) We show it only in the case where the characteristic of k is different from 2 and 3. In this case we may assume E is defined by $y^2 = x^3 + ax + b$, $a, b \in k$. An automorphism of E is then given by $(x, y) \mapsto (u^2 x, u^3 y)$ with $u \in k^\times$ satisfying $u^4 a = a$, $u^6 b = b$. If $j \neq 0, 1728$, then we have $a \neq 0, b \neq 0$, and thus $u = \pm 1$. If $j = 0$, then we have $a = 0, b \neq 0$, and thus u is a 6th root of unity. If $j = 1728$, then we have $a \neq 0, b = 0$, and thus u is a 4th root of unity.

We omit the proof of (5) and (6). □

EXAMPLE 8.42. Define an elliptic curve E over the open scheme $U_{\mathbf{Z}[\frac{1}{6}]} = \mathrm{Spec}\,\mathbf{Z}[j]\left[\frac{1}{6}, \frac{1}{j(j-12^3)}\right] \subset Y(1)_{\mathbf{Z}} = \mathbf{A}^1_{\mathbf{Z}} = \mathrm{Spec}\,\mathbf{Z}[j]$ by

$$y^2 = 4x^3 - \frac{12^3 j}{j - 12^3}x - \frac{24^3 j}{j - 12^3}. \tag{2.24}$$

As we showed in Proposition 2.15(1), the j-invariant of E equals j. Let $r \geq 3$ be an integer. The functor associating to a scheme T over $U_{\mathbf{Z}[\frac{1}{6r}]}$ the set {isomorphisms $(\mathbf{Z}/r\mathbf{Z})^2 \to E[r]_T$ of group schemes over T} is represented by a $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$-torsor $M(r)_{E, U_{\mathbf{Z}[\frac{1}{6r}]}}$. The morphism $M(r)_{E,U_{\mathbf{Z}[\frac{1}{6r}]}} \to Y(r)_{\mathbf{Z}[\frac{1}{r}]} \times_{Y(1)_{\mathbf{Z}}} U_{\mathbf{Z}[\frac{1}{6r}]}$ over $U_{\mathbf{Z}[\frac{1}{6r}]}$ defined by the universal isomorphism $(\mathbf{Z}/r\mathbf{Z})^2 \to E[r]$ is compatible with the action of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. This induces an isomorphism

$$M(r)_{E,U_{\mathbf{Z}[\frac{1}{6r}]}}/\{\pm 1\} \longrightarrow Y(r)_{\mathbf{Z}[\frac{1}{r}]} \times_{Y(1)_{\mathbf{Z}}} U_{\mathbf{Z}[\frac{1}{6r}]}$$

of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$-torsors over $U_{\mathbf{Z}[\frac{1}{6r}]}$. $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is isomorphic to the integral closure of $Y(1)_{\mathbf{Z}[\frac{1}{r}]}$ in $M(r)_{E,U_{\mathbf{Z}[\frac{1}{6r}]}}/\{\pm 1\}$.

QUESTION. Let E be the elliptic curve over $\operatorname{Spec} \mathbf{Z}[\frac{1}{2}, \lambda, \frac{1}{\lambda(1-\lambda)}]$ defined by $y^2 = x(x-1)(x-\lambda)$, and let $\alpha : (\mathbf{Z}/2\mathbf{Z})^2 \to E[2]$ be the isomorphism defined by the basis $(0,0)$, $(1,0)$. Show that the pair $(E, \alpha) \in \mathcal{M}(2)_{\mathbf{Z}[\frac{1}{2}]}\left(\operatorname{Spec} \mathbf{Z}\left[\frac{1}{2}, \lambda, \frac{1}{\lambda(1-\lambda)}\right]\right)$ defines an isomorphism $\operatorname{Spec} \mathbf{Z}[\frac{1}{2}, \lambda, \frac{1}{\lambda(1-\lambda)}] \to Y(2)_{\mathbf{Z}[\frac{1}{2}]}$, where $Y(2)_{\mathbf{Z}[\frac{1}{2}]}$ is the coarse moduli scheme of $\mathcal{M}(2)_{\mathbf{Z}[\frac{1}{2}]}$.

COROLLARY 8.43. *Let $N \geq 1$ be an integer, and let $r \geq 3$ be an integer relatively prime to N. The functor $\mathcal{M}_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ is represented by a finite scheme $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ over $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$. $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{rN}]}$ is smooth over $\mathbf{Z}[\frac{1}{rN}]$.*

The field of constants of $Y_{1,*}(N, r)_{\mathbf{Q}} = Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ is $\mathbf{Q}(\zeta_r)$.

PROOF. Let E be the universal elliptic curve over $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$. By Corollary 8.24, the functor $\mathcal{M}_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ is represented by the finite scheme $M_1(N)_E = Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ over $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$.

Since $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{Nr}]} \to Y(r)_{\mathbf{Z}[\frac{1}{Nr}]}$ is étale and $Y(r)_{\mathbf{Z}[\frac{1}{Nr}]}$ is a smooth affine curve over $\mathbf{Z}[\frac{1}{Nr}]$, $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{Nr}]}$ is also a smooth affine curve over $\mathbf{Z}[\frac{1}{Nr}]$.

The proof of the fact that $\mathbf{Q}(\zeta_r)$ is the field of constants of $Y_{1,*}(N, r)_{\mathbf{Q}} = Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ is similar to that of Lemma 8.37, and we omit it. ☐

The proofs of Theorems 8.32 and 8.34 go as follows. We first define Igusa curves and study their properties in §8.6. Then in §8.7 we study the modular curve $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ using Igusa curves and prove Theorem 8.34. Finally in §8.8, we study the modular curve $Y_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ and prove Theorem 8.32.

8.6. Igusa curves

Let p be a prime number, and let $r \geq 3$ be an integer relatively prime to p. Let E be the universal elliptic curve over $Y(r)_{\mathbf{F}_p} = Y(r)_{\mathbf{Z}[\frac{1}{r}]} \otimes \mathbf{F}_p$, and let $Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$ be the closed subscheme of $Y(r)_{\mathbf{F}_p}$ defined by the condition that E is supersingular.

LEMMA 8.44. *Let p be a prime number, and let $r \geq 3$ be an integer relatively prime to p. $Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is a Cartier divisor of $Y(r)_{\mathbf{F}_p}$ and is finite étale over $\mathbf{F}_p$.*

PROOF. We show $S = Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is étale over $\mathbf{F}_p$. It suffices to show that the absolute Frobenius morphism $F : S \to S$ is an automorphism of S of finite order. $F : S \to S$ is the endomorphism defined by sending the isomorphism class $[(E, \alpha)]$ of a pair of a supersingular elliptic curve E and a basis α of $E[r]$ to the isomorphism class $[(E^{(p)}, \alpha^{(p)})]$. Since E is supersingular, we have $\operatorname{Ker}[p] = \operatorname{Ker} F^2$. Thus, we have an isomorphism $f_E : E \to E^{(p^2)}$ satisfying $F^2 = f_E \circ [p]$. This implies that F^2 maps $[(E, \alpha)]$ to $[(E^{(p^2)}, \alpha^{(p^2)})] = [(E, \alpha \circ p)]$. Hence, if n is the order of $p \in (\mathbf{Z}/r\mathbf{Z})^\times$, F^{2n} is the identity morphism of S.

$Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is a closed subscheme that is étale over $\mathbf{F}_p$ of the smooth curve $Y(r)_{\mathbf{F}_p}$ over $\mathbf{F}_p$. Thus, $Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is a Cartier divisor of $Y(r)_{\mathbf{F}_p}$ and is finite over $\mathbf{F}_p$. ☐

COROLLARY 8.45. *Let p be a prime number, let S be a scheme over $\mathbf{F}_p$, and let E be an elliptic curve over S. E is supersingular if and only if there exists an integer $a > 0$ such that* $\operatorname{Ker}[p^a] = \operatorname{Ker} F^{2a}$.

PROOF. Since the "if" part is clear from the definition, we show the "only if" part. Since the assertion is étale local on S, we may assume there exists an isomorphism $\alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r]$, where $r \geq 3$ is an integer relatively prime to p. Let $S \to Y(r)_{\mathbf{F}_p}$ be the morphism defined by (E, α). Since $S \to Y(r)_{\mathbf{F}_p}$ factors through the closed subscheme of $Y(r)_{\mathbf{F}_p}$ defined by the closed condition $\operatorname{Ker}[p^a] = \operatorname{Ker} F^{2a}$, it suffices to show the assertion assuming S to be the closed subscheme of $Y(r)_{\mathbf{F}_p}$ defined by the condition $\operatorname{Ker}[p^a] = \operatorname{Ker} F^{2a}$. Then, similarly to the proof of Lemma 8.44, the absolute Frobenius morphism of S is an automorphism of S of finite order, and thus S is étale over $\mathbf{F}_p$. The assertion now follows from Proposition 8.2(3) (i) ⇒ (ii). ☐

LEMMA 8.46. *Let p be a prime number, let S be a scheme over $\mathbf{F}_p$, and let E be an elliptic curve over S. Let $e = a + b \geq g \geq 0$ be* *an integer, and define* $G_{(a,b)}$ *by*

$$G_{(a,b)} = \begin{cases} \operatorname{Ker}(V^aF^b : E \to E^{(p^{b-a})}) & \text{if } a \leq b, \\ \operatorname{Ker}(V^aF^b : E^{(p^{a-b})} \to E) & \text{if } a \geq b. \end{cases} \tag{8.42}$$

1. $G^{\times}_{(a,b)}$ *is a finite flat scheme of finite presentation over* S *of degree* $\varphi(p^e)$.
2. $G_{(a,b)}$ *is a cyclic subgroup scheme of order* p^e.
3. *If* P *is a generator of* $G_{(a,0)} = \operatorname{Ker} V^a$, P *has exact order* p^e *as a section of* $E^{(p^a)}$.

PROOF. (1) Let $r \geq 3$ be an integer relatively prime to p. Since the assertion is flat local on S, we may assume there is a basis α of $E[r]$ over S. Since α defines a morphism $S \to Y(r)_{\mathbf{F}_p}$, it suffices to show it assuming $S = Y(r)_{\mathbf{F}_p}$. By Lemma 8.15(1), $G = G_{(a,b)}$ is a cyclic subgroup scheme of order p^e at each point of S. By Lemma 8.25(2), $G^{\times}$ has degree $\varphi(p^e)$ at each point of S^{ord}, and degree $\leq \varphi(p^e)$ at each point of S^{ss}. By Lemma 8.44, $G^{\times}$ is a finite flat scheme of degree $\varphi(p^e)$ over a dense open subscheme $U \subset S^{\mathrm{ord}}$ of S. Thus, by Lemma A.43, $G^{\times}$ is a finite flat scheme of degree $\varphi(p^e)$ at every point of S.

(2) By (1), $G^{\times}_{(a,b)}$ is a flat covering of S and $G_{(a,b)}$ has a universal generator on $G^{\times}_{(a,b)}$.

(3) As in (1), the assertion is flat local on S. Thus, it suffices to prove, assuming that $r \geq 3$ is an integer relatively prime to p, S is $G^{\times}_{(a,0)}$ over $Y(r)_{\mathbf{F}_p}$ and P is the universal generator of $G_{(a,0)}$. Since 0 is a generator of $\operatorname{Ker} F^b$, the assertion on S^{ord} follows by applying Lemma 8.17 to the exact sequence $0 \to \operatorname{Ker} F^b \to G_{(a,b)} \to \operatorname{Ker} V^a \to 0$. Since S is flat over $Y(r)_{\mathbf{F}_p}$, there is no closed subscheme of S other than S itself that contains S^{ord} as an open subscheme. Thus, the assertion follows from Lemma 8.23. ☐

DEFINITION 8.47. Let p be a prime number, and let $a \geq 0$, $M \geq 1$, $r \geq 3$ be integers. Assume M, r and p are pairwise relatively prime. Let E be the universal elliptic curve over $Y_{1,*}(M,r)_{\mathbf{F}_p}$. The finite flat scheme

$$G^{\times}_{(a,0)} = (\operatorname{Ker} V^a : E^{(p^a)} \to E)^{\times}$$

of degree $\varphi(p^a)$ over $Y_{1,*}(M,r)_{\mathbf{F}_p}$ is called the *Igusa curve* and is denoted by $\operatorname{Ig}(Mp^a, r)_{\mathbf{F}_p}$.

If $a = 0$, we have $\mathrm{Ig}(M, r)_{\mathbf{F}_p} = Y_{1,*}(M, r)_{\mathbf{F}_p}$. The Igusa curve $\mathrm{Ig}(Mp^a, r)_{\mathbf{F}_p}$ represents the functor that associates to a scheme T over $\mathbf{F}_p$ the set

$$\left\{\begin{array}{l}\text{isomorphism classes of quadruples } (E, P, P', \alpha), \text{ where} \\ E \text{ is an elliptic curve over } T,\ P \text{ is a generator of } G_{(a,0)} = \\ \operatorname{Ker} V^a \subset E^{(p^a)},\ P' \text{ is a section of } E \text{ of exact order } M, \\ \text{and } \alpha : (\mathbf{Z}/r\mathbf{Z})^2 \to E[r] \text{ is an isomorphism.}\end{array}\right\}. \tag{8.43}$$

If P is the universal generator of the cyclic subgroup scheme $G_{(a,0)}$ over the Igusa curve $\mathrm{Ig}(Mp^a, r)_{\mathbf{F}_p}$, we denote by $\mathrm{Ig}(Mp^a, r)^{P=0}_{\mathbf{F}_p}$ the closed subscheme of $\mathrm{Ig}(Mp^a, r)_{\mathbf{F}_p}$ defined by the closed condition $P = 0$.

LEMMA 8.48. *Let p be a prime number, and let $a \geq 0$, $M \geq 1$, $r \geq 3$ be integers. Suppose M, r, p are pairwise relatively prime.*

(1) *The Igusa curve $\mathrm{Ig}(Mp^a, r)_{\mathbf{F}_p}$ is a smooth affine curve over $\mathbf{F}_p$.*
(2) *The natural morphism $\mathrm{Ig}(Mp^a, r)_{\mathbf{F}_p} \to Y_{1,*}(M, r)_{\mathbf{F}_p}$ is étale over $Y_{1,*}(M, r)^{\mathrm{ord}}_{\mathbf{F}_p}$.*
(3) *Suppose $a \geq 1$. The closed subscheme $\mathrm{Ig}(Mp^a, r)^{P=0}_{\mathbf{F}_p}$ is the reduced part of $\mathrm{Ig}(Mp^a, r)^{\mathrm{ss}}_{\mathbf{F}_p}$. The morphism $\mathrm{Ig}(Mp^a, r)^{P=0}_{\mathbf{F}_p} \to Y_{1,*}(M, r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is an isomorphism.*

PROOF. The morphism $\mathrm{Ig}(Mp^a, r)_{\mathbf{F}_p} \to Y_{1,*}(M, r)_{\mathbf{F}_p}$ is the base change of the morphism $\mathrm{Ig}(p^a, r)_{\mathbf{F}_p} \to Y(r)_{\mathbf{F}_p}$ by the étale morphism $Y_{1,*}(M, r)_{\mathbf{F}_p} \to Y(r)_{\mathbf{F}_p}$. Thus, it suffices to show them assuming $M = 1$.

(2) Since $\operatorname{Ker} V^a$ is étale over $Y(r)^{\mathrm{ord}}_{\mathbf{F}_p}$, the morphism $\mathrm{Ig}(p^a, r)_{\mathbf{F}_p} \to Y(r)_{\mathbf{F}_p}$ is étale over $Y(r)^{\mathrm{ord}}_{\mathbf{F}_p}$.

(3) We show $\mathrm{Ig}(p^a, r)^{P=0}_{\mathbf{F}_p} \subset \mathrm{Ig}(p^a, r)^{\mathrm{ss}}_{\mathbf{F}_p}$. To do so, it suffices to show that the universal elliptic curve E over $S = \mathrm{Ig}(p^a, r)^{P=0}_{\mathbf{F}_p}$ is supersingular. Since $P = 0$ is a generator of $\operatorname{Ker} V^a \subset E^{(p^a)}$ over S, we have $\operatorname{Ker} V^a = \operatorname{Ker} F^a$, and thus $\operatorname{Ker}[p^a] = \operatorname{Ker} F^{2a} \subset E$. Hence, by Corollary 8.45, E is supersingular. Since we have $\mathrm{Ig}(p^a, r)^{P=0}_{\mathbf{F}_p} \subset \mathrm{Ig}(p^a, r)^{\mathrm{ss}}_{\mathbf{F}_p}$, we obtain a morphism $\mathrm{Ig}(p^a, r)^{P=0}_{\mathbf{F}_p} \to Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$. This is an isomorphism since the inverse morphism $Y(r)^{\mathrm{ss}}_{\mathbf{F}_p} \to \mathrm{Ig}(p^a, r)^{P=0}_{\mathbf{F}_p}$ is defined by sending (E, α) to $(E, 0, \alpha)$.

For a supersingular elliptic curve over a field k of characteristic p, the only section $P \in E(k)$ that generates $\operatorname{Ker} V^a$ is $P = 0$. Thus,

$\mathrm{Ig}(p^a,r)^{P=0}_{\mathbf{F}_p} \to \mathrm{Ig}(p^a,r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is surjective. Since $\mathrm{Ig}(p^a,r)^{P=0}_{\mathbf{F}_p} = Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is reduced, this is the reduced part of $\mathrm{Ig}(p^a,r)^{\mathrm{ss}}_{\mathbf{F}_p}$.

(1) It suffices to show it assuming $a \geq 1$. Let E be the universal elliptic curve over $\mathrm{Ig}(p^a,r)_{\mathbf{F}_p}$. By Lemma B.2(1), the 0-section of E is a Cartier divisor of E. Thus, the closed subscheme $\mathrm{Ig}(p^a,r)^{P=0}_{\mathbf{F}_p} \subset \mathrm{Ig}(p^a,r)_{\mathbf{F}_p}$ is defined locally by a principal ideal. Since $\mathrm{Ig}(p^a,r)_{\mathbf{F}_p}$ is flat over $Y(r)_{\mathbf{F}_p}$, $\mathrm{Ig}(p^a,r)^{P=0}_{\mathbf{F}_p}$ is a Cartier divisor of $\mathrm{Ig}(p^a,r)_{\mathbf{F}_p}$ by Lemma A.40. $\mathrm{Ig}(p^a,r)^{P=0}_{\mathbf{F}_p}$ is étale over $\mathbf{F}_p$. Thus, by Lemma B.2(2), $\mathrm{Ig}(p^a,r)_{\mathbf{F}_p}$ is smooth over $\mathbf{F}_p$ on a neighborhood of $\mathrm{Ig}(p^a,r)^{P=0}_{\mathbf{F}_p}$. Since the complementary open subscheme $\mathrm{Ig}(p^a,r)^{\mathrm{ord}}_{\mathbf{F}_p}$ of $\mathrm{Ig}(p^a,r)^{P=0}_{\mathbf{F}_p}$ is étale over $Y(r)^{\mathrm{ord}}_{\mathbf{F}_p}$, it is smooth over $\mathbf{F}_p$. Thus, $\mathrm{Ig}(p^a,r)_{\mathbf{F}_p}$ is smooth everywhere over $\mathbf{F}_p$. □

Let $0 \leq a \leq e$ be integers, and let $N = Mp^e$. Let $r \geq 3$ be an integer, and suppose M, r and p are pairwise relatively prime. For an elliptic curve E over a scheme T over $\mathbf{F}_p$, its section P' of exact order M and a basis α of $E[r]$, $P'^{(p^a)}$ and $\alpha^{(p^a)}$ define a section of $E^{(p^a)}$ of exact order M and a basis of $E^{(p^a)}[r]$, respectively. Thus, by Lemma 8.46(3), a morphism $j_a : \mathrm{Ig}(Mp^a,r)_{\mathbf{F}_p} \to Y_{1,*}(N,r)_{\mathbf{F}_p} \subset Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is defined by sending the isomorphism class $[(E,P,P',\alpha)]$ to the isomorphism class $[(E^{(p^a)},(P,P'^{(p^a)}),\alpha^{(p^a)})]$.

PROPOSITION 8.49. *Let p be a prime, and let $e \geq 0$, $M \geq 1$, $r \geq 3$ be integers. Suppose M, r and p are pairwise relatively prime. Let $N = Mp^a$.*

(1) *For $0 \leq a \leq e$, the morphism*

$$j_a : \mathrm{Ig}(Mp^a,r)_{\mathbf{F}_p} \longrightarrow Y_{1,*}(N,r)_{\mathbf{F}_p} \tag{8.44}$$

is a closed immersion.

(2) *For $0 \leq a \leq e$, if we denote by C_a the image of the closed immersion $j_a : \mathrm{Ig}(Mp^a,r)_{\mathbf{F}_p} \to Y_{1,*}(N,r)_{\mathbf{F}_p}$, then we have $Y_{1,*}(N,r)_{\mathbf{F}_p} = \bigcup_{a=0}^{e} C_a$. For each $0 \leq a \leq e$, the inclusion $C_a^{\mathrm{ss}} \to Y_{1,*}(N,r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is bijective.*

(3) *For $0 \leq a < a' \leq e$, the intersection $C_a \times_{Y_{1,*}(N,r)_{\mathbf{F}_p}} C_{a'}$ is C_a^{ss}.*

PROOF. Similarly to the proof of Lemma 8.48, it suffices to show it in the case where $M = 1$, $N = p^e$, $e \geq 1$.

(1) Let $0 \leq a \leq e$ be integers. In general, if S is a scheme over $\mathbf{F}_p$, E is an elliptic curve over S, and P is a section of E over S, then by Lemma 8.23, the condition that P has exact order p^a is a closed

condition. Let T be the closed subscheme of S defined by this closed condition, and let $\langle P\rangle_{p^a} = \sum_{i=0}^{p^a-1}[iP]$ over T. The condition that the kernel of the dual of $E_T \to E' = E_T/\langle P\rangle_{p^a}$ equals

$$\operatorname{Ker}(F^a : E' \to E'^{(p^a)})$$

is a closed condition on T.

Define a closed subscheme C_a of $Y_{1,*}(N,r)_{\mathbf{F}_p}$ by the closed condition:

(8.45) The universal generator P has exact order p^a, and the kernel of the dual of $E \to E/\langle P\rangle_{p^a}$ equals $\operatorname{Ker} F^a$.

The morphism $j_a : \operatorname{Ig}(p^a,r)_{\mathbf{F}_p} \to Y_{1,*}(N,r)_{\mathbf{F}_p}$ defines a morphism $\operatorname{Ig}(p^a,r)_{\mathbf{F}_p} \to C_a$. Define a morphism $C_a \to \operatorname{Ig}(p^a,r)_{\mathbf{F}_p}$ by sending (E,P,α) to the isomorphism class of $(E', P,$ the image of $\alpha \circ p^{-a})$. Since $E = E'^{(p^a)}$ over C_a, and $V^a \circ F^a = [p^a]$, this is the inverse morphism of $\operatorname{Ig}(p^a,r)_{\mathbf{F}_p} \to C_a$. Thus, the morphism $\operatorname{Ig}(p^a,r)_{\mathbf{F}_p} \to C_a$ is an isomorphism, and $j_a : \operatorname{Ig}(p^a,r)_{\mathbf{F}_p} \to Y_{1,*}(N,r)_{\mathbf{F}_p}$ is a closed immersion.

(2) For a rational point $[(E,P,\alpha)] \in Y_{1,*}(N,r)(k)$ over an algebraically closed field of characteristic p, let p^a be the order of $P \in E(k)$. Then we have $[(E,P,\alpha)] \in C_a(k)$. Thus, we have $Y_{1,*}(N,r)_{\mathbf{F}_p} = \bigcup_{a=0}^{e} C_a$. If E is supersingular, then $P = 0$. In this case, for any $0 \leq a \leq e$, we have $[(E,P,\alpha)] \in C_a(k)$, and thus the mapping $\operatorname{Ig}(p^a,r)^{\mathrm{ss}}_{\mathbf{F}_p} \to Y_{1,*}(N,r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is bijective.

(3) Let (E,P,α) be an elliptic curve with the universal level structure over the intersection $C_a \times_{Y_{1,*}(N,r)_{\mathbf{F}_p}} C_{a'}$. Consider $E \to E' = E/\langle P\rangle_{p^a} \to E'' = E/\langle P\rangle_{p^{a'}}$. Since $p^aP = 0$, we have $\operatorname{Ker}(E' \to E'') = \operatorname{Ker} F^{a'-a}$. Since the kernel of its dual is also $\operatorname{Ker} F^{a'-a}$, we have $E'[p^{a'-a}] = \operatorname{Ker} F^{2(a'-a)}$. Thus, by Corollary 8.45, E' is supersingular. Hence, $E \simeq E'^{(p^a)}$ is also supersingular. The intersection $C_a \cap C_{a'}$ is a closed subscheme of C_a^{ss}.

We now show $C_a^{\mathrm{ss}} \subset C_a \cap C_{a'}$. Let (E,P,α) be the universal elliptic curve with level structure over C_a^{ss}. Since $\operatorname{Ker}[p^a] = \operatorname{Ker} F^{2a}$, the kernel of $E \to E' = E/\langle P\rangle_{p^a}$ equals $\operatorname{Ker} F^a$. Since $p^aP = 0$, $\langle P\rangle_{p^{a'}} = \sum_{i=0}^{p^{a'}-1}[iP]$ is the inverse image of $\operatorname{Ker} F^{a'-a}$ by $E \to E'$. Since $\langle P\rangle_{p^{a'}} = \operatorname{Ker} F^{a'}$ and $\operatorname{Ker}[p^{a'}] = \operatorname{Ker} F^{2a'}$, we have $C_a^{\mathrm{ss}} \subset C_{a'}$. □

8.7. Modular curve $Y_1(N)_{\mathbf{Z}}$

PROPOSITION 8.50. *Let $N \geq 1$ be an integer, and let $r \geq 3$ be an integer relatively prime to N. The fine moduli scheme $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ is a regular affine curve over $\mathbf{Z}[\frac{1}{r}]$. The natural morphism $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_1(r)_{\mathbf{Z}[\frac{1}{r}]}$ is finite flat of degree $\varphi(N)\psi(N)$.*

PROOF. Let p be a prime number. We first show $Y_{1,*}(p^e, r)_{\mathbf{Z}[\frac{1}{r}]}$ is regular in the case where $N = p^e > 1$. Since $Y_{1,*}(p^e, r)_{\mathbf{Z}[\frac{1}{pr}]}$ is smooth over $\mathbf{Z}[\frac{1}{pr}]$, it suffices to examine a neighborhood of $Y_{1,*}(p^e, r)_{\mathbf{F}_p}$. Let $S = Y_{1,*}(p^e, r)_{\mathbf{Z}[\frac{1}{r}]}$.

For $0 \leq a \leq e$, define a closed subscheme D_a of $S = Y_{1,*}(p^e, r)_{\mathbf{Z}[\frac{1}{r}]}$ as follows. Let P be a universal element over S of exact order p^e. If $a < e$, let D_a be the closed subscheme defined by the condition $p^a P = 0$, and define $D_e = Y_{1,*}(p^e, r)_{\mathbf{F}_p}$. If $a < e$, D_a is the pullback of the 0-section by the morphism $S \to E$ defined by $p^a P$. Thus, by Lemma B.2(1), D_a is defined locally by a principal ideal. If $a = e$, D_e is the principal ideal (p).

We study the relation between D_a and the image C_a of the closed immersion $j_a : \mathrm{Ig}(p^a, r) \to S$ (8.44). Let $D_a^{\text{ét}}$ be the open subscheme of D_a defined by the condition that the divisor $\sum_{i=0}^{p^a-1}[iP]$ is étale over D_a.

LEMMA 8.51. (1) $C_0 = D_0$.
(2) *If $0 < a \leq e$, we have $C_a^{\text{ord}} = D_a^{\text{ét}}$.*

PROOF. (1) C_0 is the closed subscheme of $Y_{1,*}(p^e, r)_{\mathbf{Z}[\frac{1}{r}]}$ defined by the condition $p = 0$ and $P = 0$, and D_0 is the closed subscheme defined by the condition $P = 0$. Since D_0 is a scheme over $\mathbf{F}_p$ by Lemma 8.22, we have $C_0 = D_0$.

(2) On C_a^{ord}, we have $p^a P = 0$, and

$$\langle P \rangle_{p^a} = \mathrm{Ker}(V^a : E = E'^{(p^a)} \to E')$$

is étale. Thus, we have $C_a^{\text{ord}} \subset D_a^{\text{ét}}$. Conversely, on $D_a^{\text{ét}}$, $\langle P \rangle_{p^a} = \sum_{i=0}^{p^a-1}[iP]$ is an étale closed subgroup scheme. By Lemma 8.17, $p^a P = 0$ has exact order p^{e-a}. We have $p = 0$ on $D_a^{\text{ét}}$, by Lemma 8.22 if $a < e$, and by definition if $a = e$. Since $\langle P \rangle_{p^a}$ is étale, the kernel of the dual $E/\langle P \rangle_{p^a} \to E$ equals $\mathrm{Ker}\, F^a$ by Lemma 8.4, and $\langle P \rangle_{p^a} = \mathrm{Ker}\, V^a$. Thus, $D_a^{\text{ét}} \subset C_a^{\text{ord}}$. □

We show $S - S^{\mathrm{ss}}_{\mathbf{F}_p}$ is regular. $S_{\mathbf{Z}[\frac{1}{p}]} \to Y(r)_{\mathbf{Z}[\frac{1}{pr}]}$ is finite étale of degree $\varphi(N)\psi(N)$. Thus, by Lemmas 8.25 and A.43, we see that $S - S^{\mathrm{ss}}_{\mathbf{F}_p} \to Y(r)_{\mathbf{Z}[\frac{1}{r}]} - Y(r)^{\mathrm{ss}}_{\mathbf{F}_p}$ is finite flat. Since $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is smooth over $\mathbf{Z}[\frac{1}{r}]$, $S - S^{\mathrm{ss}}_{\mathbf{F}_p}$ is also finite flat over $\mathbf{Z}[\frac{1}{r}]$. Since D_a is defined by a principal ideal locally on S, C^{ord}_a is a Cartier divisor of $S - S^{\mathrm{ss}}_{\mathbf{F}_p}$ by Lemmas 8.51 and A.40. By Lemma 8.48, C_a is a regular subscheme of S. Since $S_{\mathbf{F}_p} = \bigcup_{a=0}^{e} C_a$ by Proposition 8.49(2), $S - S^{\mathrm{ss}}_{\mathbf{F}_p}$ is regular. Applying Corollary A.42 to the closed immersion $S^{\mathrm{ss}}_{\mathbf{F}_p} \subset D_0 = C_0 \to S$, we see that S is regular on a neighborhood of $S^{\mathrm{ss}}_{\mathbf{F}_p}$.

$S \to Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is finite flat of degree $\varphi(N)\psi(N)$ except for $S^{\mathrm{ss}}_{\mathbf{F}_p}$. Since both S and $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ are regular, $S \to Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is finite flat everywhere and of degree $\varphi(N)\psi(N)$ by Proposition A.13(2). This proves that $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is a regular affine curve over $\mathbf{Z}[\frac{1}{r}]$ in the case $N = p^e$.

We now show it for general N. If $N = \prod_{p|N} p^{e_p}$, $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ has an open covering $\bigcup_{p|N} Y_{1,*}(N,r)_{\mathbf{Z}[\frac{p^{e_p}}{rN}]}$. Since the natural morphism $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{p^{e_p}}{rN}]} \to Y_{1,*}(p^{e_p},r)_{\mathbf{Z}[\frac{p^{e_p}}{rN}]}$ is finite étale of degree $\varphi(N/p^{e_p})\psi(N/p^{e_p})$, the proof is reduced to the case $N = p^e$. □

PROOF OF THEOREM 8.34. (1) Let $r \geq 3$ be an integer relatively prime to N. Consider the action of the group $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ on $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. As in Proposition 2.23, the quotient $Y_1(N)_{\mathbf{Z}[\frac{1}{r}]}$ of $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ by the action of the group $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ is the coarse moduli scheme of the restriction of the functor $\mathcal{M}_1(N)$ over $\mathbf{Z}$ to $\mathbf{Z}[\frac{1}{r}]$. By Proposition 8.50, $Y_1(N)_{\mathbf{Z}[\frac{1}{r}]}$ is a normal affine curve over $\mathbf{Z}[\frac{1}{r}]$. Since the coarse moduli scheme $Y_1(N)_{\mathbf{Z}}$ is obtained by patching together $Y_1(N)_{\mathbf{Z}[\frac{1}{r}]}$ with $(N,r) = 1$, it is a normal affine curve over $\mathbf{Z}$.

If $N \geq 4$, then by Lemma 8.38(2), the action of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ on $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is free. Similarly to the proof of Lemma 8.37, $Y_1(N)_{\mathbf{Z}[\frac{1}{Nr}]}$ represents the functor $[\mathcal{M}_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{N}r]}/\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})]$ by Lemmas A.31, and A.33. Thus, by Corollary 8.39(2), $Y_1(N)_{\mathbf{Z}[\frac{1}{Nr}]}$ is a fine moduli scheme of $\mathcal{M}_1(N)_{\mathbf{Z}[\frac{1}{Nr}]}$.

We now show $Y_1(N)_{\overline{\mathbf{Q}}}$ is a smooth connected affine curve over $\overline{\mathbf{Q}}$. It suffices to show the Riemann surface $Y_1(N)^{\mathrm{an}}$ defined by $Y_1(N)_{\mathbf{Q}}$ is connected. Let $\Gamma_1(N)$ be the subgroup of $\mathrm{SL}_2(\mathbf{Z})$ defined by

$$(8.46)\quad \Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, a \equiv 1 \bmod N, c \equiv 0 \bmod N \right\},$$

and consider the action of $\Gamma_1(N)$ on the upper half-plane $H = \{\tau \in \mathbf{C} \mid \operatorname{Im}\tau > 0\}$. As in Corollary 2.66, we obtain an isomorphism of Riemann surfaces

$$\Gamma_1(N)\backslash H \longrightarrow Y_1(N)^{\mathrm{an}}. \tag{8.47}$$

This implies $Y_1(N)^{\mathrm{an}}$ is connected, and $Y_1(N)_{\overline{\mathbf{Q}}}$ is a smooth connected affine curve over $\overline{\mathbf{Q}}$. Hence, $Y_1(N)_{\mathbf{Q}}$ is connected, and so is $Y_1(N)_{\mathbf{Z}}$.

(2) $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_1(r)_{\mathbf{Z}[\frac{1}{r}]}$ is a finite surjective morphism of two-dimensional normal schemes by Proposition 8.50. Thus, the induced morphism $Y_1(N)_{\mathbf{Z}} \to Y(1)_{\mathbf{Z}}$ is also a finite surjective morphism of two-dimensional normal schemes. Since $Y(1)_{\mathbf{Z}}$ is isomorphic to $\mathbf{A}^1_{\mathbf{Z}}$, it is thus regular. Hence, $Y_1(N)_{\mathbf{Z}} \to Y(1)_{\mathbf{Z}}$ is finite flat by Proposition A.13(2).

$Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_1(N)_{\mathbf{Z}[\frac{1}{r}]}$ is a Galois covering whose Galois group equals $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ for $N \geq 3$ and $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/\{\pm 1\}$ for $N = 1, 2$ by Lemma 8.41(2). Since the degree of $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_1(r)_{\mathbf{Z}[\frac{1}{r}]}$ is $\psi(N)\varphi(N)$ by Proposition 8.50, the degree of $Y_1(N)_{\mathbf{Z}[\frac{1}{r}]} \to Y(1)_{\mathbf{Z}[\frac{1}{r}]}$ equals $\psi(N)\varphi(N)/2$ for $N \geq 3$, and $\psi(N)\varphi(N)$ for $N = 1, 2$.

(3) Since $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is a smooth affine curve over $\mathbf{Z}[\frac{1}{r}]$, its quotient $Y_1(N)_{\mathbf{Z}[\frac{1}{r}]}$ is a smooth affine curve by Proposition B.10(1). Suppose $p \nmid N$. If $N \geq 4$, $Y_1(N)_{\mathbf{Z}[\frac{1}{N}]}$ is a fine moduli scheme, and thus $Y_1(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p$ is a fine moduli scheme of the restriction $\mathcal{M}_1(N)_{\mathbf{F}_p}$. As for the action of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ on $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$, the inertia group at the generic point of each irreducible component of each fiber is a subgroup of $\{\pm 1\}$ by Lemma 8.41(2). If $N > 2$, we have $-P \neq P$ for an element P of order N, and thus the inertia group equals 1. If $N \leq 2$, the inertia group is $\{\pm 1\}$. Hence, by Corollary B.11(1), $Y_1(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p$ is the quotient of $Y_{1,*}(N,r)_{\mathbf{F}_p}$ by $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$, and it is a coarse moduli scheme of the restriction of the functor $\mathcal{M}_1(N)_{\mathbf{F}_p}$. □

We present some consequences of Proposition 8.50.

PROPOSITION 8.52. *Let S be a scheme, and let E be an elliptic curve over S. Let $N \geq 1$ be an integer.*

(1) *The finite scheme $M_1(N)_E$ over S is flat of finite presentation over S of degree $\varphi(N)\psi(N)$. The scheme $M_1(N)_E$ is a Cartier divisor of E.*

If $N = N'N''$ with $(N', N'') = 1$, then we have $M_1(N)_E = M_1(N')_E \times_S M_1(N'')_E$. If $N = p^e$ with $e \geq 1$, then we have an *equality of Cartier divisors*

(8.48)

$$M_1(N)_E = \big[\mathrm{Ker}[p^e]\big] - \big[\mathrm{Ker}[p^{e-1}]\big] = E[p^e] \underset{[p^{e-1}]\searrow E[p]}{\times} (E[p] - [0]).$$

(2) *Let P be a section of E of exact order N. Let $G = \langle P \rangle = \sum_{a \in \mathbf{Z}/N\mathbf{Z}} [aP]$. Then, we have $G^\times = \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} [aP]$.*

PROOF. (1) It suffices to show the following case: $N = p^e$, $r \geq 3$ an integer relatively prime to N, $S = Y(r)_{\mathbf{Z}[\frac{1}{r}]}$, and E the universal elliptic curve over S. In this case, we have $M_1(N)_E = Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$. By Proposition 8.50, $M_1(N)_E \to S$ is finite flat of degree $\varphi(N)\psi(N)$.

We show (8.48). Since S is flat over $\mathbf{Z}$, it suffices to apply Corollary A.44 to $U = S[1/p]$, $A = M_1(N)_E$, $B = \big[\mathrm{Ker}[p^e]\big] - \big[\mathrm{Ker}[p^{e-1}]\big]$, and $E[p^e] \underset{[p^{e-1}]\searrow E[p]}{\times} (E[p] - [0])$.

(2) We may assume S and E as above. Let P be the universal generator over $T = M_1(N)_E$. Since $T = M_1(N)_E$ is flat over $\mathbf{Z}$, it suffices to apply Corollary A.44 to the closed subscheme $A = G^\times$ of E_T and $B = \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^\times} [aP]$. □

COROLLARY 8.53. *Let S be a scheme, and let E be an elliptic curve over S. Let G be a closed subgroup scheme of E finite flat over S of degree N.*

(1) *The following conditions* (i) *and* (ii) *are equivalent.*
   (i) *G is a cyclic subgroup scheme of order N.*
   (ii) *The scheme $G^\times$ of generators of G is a finite flat scheme over S of degree $\varphi(N)$.*

(2) *The condition for a scheme T over S that G_T is a cyclic subgroup scheme of E_T is a closed condition on S.*

PROOF. (1) The proof of (ii) ⇒ (i) is similar to the proof of Lemma 8.46(2). We show (i) ⇒ (ii). Since the assertion is flat local, we may assume there exists a section of exact order N satisfying $G = \langle P \rangle$ by Definition 8.13. In this case the assertion follows easily from Proposition 8.52(2).

(2) By (1), the condition that G_T is a cyclic subgroup scheme of E_T is equivalent to the condition that $G_T^\times$ is a finite flat scheme on T of degree $\varphi(N)$. Moreover, by Proposition 8.52(2) and Nakayama's lemma, the quasi-coherent sheaf $\mathcal{O}_{G^\times}$ over S is generated by $\varphi(N)$ sections locally on S. Hence, by Corollary A.38, this condition is a closed condition. □

8.8. Modular curve $Y_0(N)_{\mathbf{Z}}$

PROPOSITION 8.54. *Let S be a scheme, and let E be an elliptic curve over S. Let $N \geq 1$ an integer.*

The functor $\mathcal{M}_0(N)_E$ over S is represented by a finite flat scheme of finite presentation $M_0(N)_E$ over S of degree $\psi(N)$. The natural morphism $M_1(N)_E \to M_0(N)_E$ is finite flat of finite presentation of degree $\varphi(N)$. If N is invertible on S, $M_0(N)_E$ is étale over S.

We first show the following lemma.

LEMMA 8.55. *Let S be a scheme, let E be an elliptic curve over S. Let $N \geq 1$ be an integer. The functor N-Isog_E defined by associating to a scheme T over S the set*

$$N\text{-}\mathrm{Isog}_E(T) = \left\{ \begin{array}{l} \textit{closed subgroup scheme of } E_T \textit{ that is a finite} \\ \textit{flat scheme of finite presentation of degree } N \\ \textit{as a scheme over } T. \end{array} \right\}$$

is represented by a finite scheme $T_{N,E}$ over S.

PROOF. The functor that associates to a scheme T over S the set {locally free quotient $\mathcal{O}_T$-module of rank N of the locally free $\mathcal{O}_T$-module $\mathcal{O}_{E[N]\times T}$} is represented by the Grassmannian scheme denoted by $\mathrm{Grass}(\mathcal{O}_{E[N]}, N)$, which is a proper scheme over S. If $G \subset E_T$ is a closed subgroup scheme flat finite of finite presentation of degree N as a scheme over T, then $\mathcal{O}_G$ is a locally free quotient $\mathcal{O}_T$-modules of rank N of $\mathcal{O}_{E[N]\times_S T}$. Thus, as in the proof of Lemma 8.23, the functor N-Isog_E is represented by a closed subscheme $T_{N,E}$ of the Grassmannian scheme $\mathrm{Grass}(\mathcal{O}_{E[N]}, N)$.

We show $T_{N,E}$ is finite over S. Since $T_{N,E}$ is proper over S, it suffices to show, by Corollary A.9, that each geometric fiber is finite. We may assume $S = \mathrm{Spec}\, k$, k is an algebraically closed field of characteristic $p > 0$, and $N = p^e$. If E is supersingular, then we have $G = \mathrm{Ker}\, F^e$ by Proposition 8.2. If E is ordinary, we have $E[N] \simeq \mathbf{Z}/p^e\mathbf{Z} \times \mu_{p^e}$, and G is of the form $\mathbf{Z}/p^a\mathbf{Z} \times \mu_{p^b}$, $a + b = e$, and there are $e + 1$ of such G. ☐

PROOF OF PROPOSITION 8.54. We show $\mathcal{M}_0(N)_E$ is representable. Let $G_{M_0(N)_E} \subset E_{M_0(N)_E}$ be the universal closed subgroup scheme. Applying Corollary 8.53(2) to $G_{T_{N,E}} \subset E_{T_{N,E}}$, we see that $\mathcal{M}_0(N)_E$ is represented by a closed subscheme $M_0(N)_E$ of $T_{N,E}$.

We now show $M_1(N)_E \to M_0(N)_E$ is finite flat of degree $\varphi(N)$. Let $G_{M_0(N)_E} \subset E_{M_0(N)_E}$ be the universal cyclic subgroup scheme of degree N. Then, since $M_1(N)_E = G^\times_{M_0(N)_E}$, $M_1(N)_E \to M_0(N)_E$ is finite flat of degree $\varphi(N)$ by Corollary 8.53(1). Since $M_1(N)_E$ is finite flat over S of degree $\varphi(N)\psi(N)$ by Proposition 8.52(1), $M_0(N)_E$ is also finite flat over S of degree $\psi(N)$.

Assuming N is invertible on S, we show $M_0(N)_E$ is étale over S. Since the assertion is étale local on S, we may assume $E[N]$ is isomorphic to $(\mathbf{Z}/N\mathbf{Z})^2$. In this case, we have, by Corollary 8.10, $M_0(N)_E = \coprod_{C\text{:cyclic subgroup of}(\mathbf{Z}/N\mathbf{Z})^2\text{ of order }N} S$, and the assertion is now clear. ☐

COROLLARY 8.56. *Let $N \geq 1$ be an integer, and let $r \geq 3$ be an integer relatively prime to N. The functor $\mathcal{M}_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ is represented by a regular finite flat scheme $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ over $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ of degree $\psi(N)$. $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{rN}]}$ is smooth over $\mathbf{Z}[\frac{1}{rN}]$.*

The field of constants of $Y_{0,*}(N,r)_{\mathbf{Q}} = Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ is $\mathbf{Q}(\zeta_r)$.

PROOF. Let E be the universal elliptic curve over $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$. The functor $\mathcal{M}_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is represented by $M_0(N)_E = Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. This is a finite flat scheme over $Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ of degree $\psi(N)$. By Proposition 8.54, $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} = M_1(N)_E \to Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} = M_0(N)_E$ is faithfully flat. Since $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is regular, so is $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ by Proposition A.13(1). Since $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{rN}]}$ is étale over $Y(r)_{\mathbf{Z}[\frac{1}{rN}]}$, it is smooth over $\mathbf{Z}[\frac{1}{rN}]$.

We omit the proof that the field of constants of $Y_{0,*}(N,r)_{\mathbf{Q}} = Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ equals $\mathbf{Q}(\zeta_r)$ because it is similar to that of Lemma 8.37. ☐

Let p be a prime number, $N = Mp^e$ with $(p, M) = 1$, $e \geq 1$ and integer, and let $r \geq 3$ be an integer relatively prime to N. Let S be a scheme over $\mathbf{F}_p$, and let E be an elliptic curve over S. Then, by Lemma 8.46(2), for $e = a + b \geq a \geq 0$,

$$G_{(a,b)} = \mathrm{Ker}(V^a F^b : E \to E^{(p^{b-a})})$$

is a cyclic subgroup scheme of E of order p^e if $a \leq b$, and

$$G_{(a,b)} = \mathrm{Ker}(V^a F^b : E^{(p^{a-b})} \to E)$$

is a cyclic subgroup scheme of $E^{(p^{a-b})}$ of order p^e if $a \geq b$. Define a morphism of schemes $j_a : Y_{0,*}(M,r)_{\mathbf{F}_p} \to Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ by

$[(E,C,\alpha)] \mapsto [(E,(G_{(a,b)},C),\alpha)]$ if $a \leq b$, and by $[(E,C,\alpha)] \mapsto [(E^{(p^{a-b})},(G_{(a,b)},C^{(p^{a-b})}),\alpha^{(p^{a-b})})]$ if $a \geq b$.

PROPOSITION 8.57. *Let p be a prime number, let $N = Mp^e$ with $(p,M) = 1$ an integer, and let $r \geq 3$ be an integer relatively prime to N.*

(1) *For $0 \leq a \leq e$, the morphism*

$$j_a : Y_{0,*}(M,r)_{\mathbf{F}_p} \longrightarrow Y_{0,*}(N,r)_{\mathbf{F}_p} \tag{8.49}$$

is a closed immersion.

(2) *For $0 \leq a \leq e$, let C_a be the image of the closed immersion $j_a : Y_{0,*}(M,r)_{\mathbf{F}_p} \to Y_{0,*}(N,r)_{\mathbf{F}_p}$. Then, we have $Y_{0,*}(N,r)_{\mathbf{F}_p} = \bigcup_{a=0}^{e} C_a$, and the inclusion $C_a^{\mathrm{ss}} \to Y_{0,*}(N,r)_{\mathbf{F}_p}^{\mathrm{ss}}$ is a bijection.*

The multiplicities of C_0 and of C_e in $Y_{0,*}(N,r)_{\mathbf{F}_p}$ are 1.

(3) *If $0 \leq a \leq e$ and $0 \leq a' \leq e$ with $a \neq a'$, then the intersection $C_a \cap C_{a'} = C_a \times_{Y_{0,*}(N,r)_{\mathbf{F}_p}} C_{a'}$ equals $C_a^{\mathrm{ss}} = C_{a'}^{\mathrm{ss}}$.*

PROOF. As in the proof of Proposition 8.49, it suffices to show the assertions when $M = 1$ and $N = p^e \geq 1$.

(1) We first show it in the case $a \leq b = e - a$. Let G be the universal cyclic subgroup scheme of order p^e over $Y_{0,*}(N,r)_{\mathbf{F}_p}$. For an integer $0 \leq a \leq b = e - a$, define a closed subscheme of $Y_{0,*}(N,r)_{\mathbf{F}_p}$ by the closed condition

$$G = \operatorname{Ker}\bigl(V^a F^b : E \to E^{(p^{b-a})}\bigr). \tag{8.50}$$

The morphism $j_a : Y(r)_{\mathbf{F}_p} \to Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ defines an isomorphism $Y(r)_{\mathbf{F}_p} \to C_a$ by definition. Thus, $j_a : Y(r)_{\mathbf{F}_p} \to Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is a closed immersion.

If $b = e - a \leq a$, a similar proof works if we define C_a by the closed condition

(8.51) the kernel $\operatorname{Ker}(E' \to E)$ of the dual of $E \to E' = E/G$ equals $\operatorname{Ker}(V^b F^a : E' \to E'^{(p^{a-b})})$.

(2) Let k be an algebraically closed field of characteristic p, let $[(E,G,\alpha)] \in Y_{0,*}(N,r)(k)$ be a k-rational point, and let p^a be the order of $G(k)$. If E is supersingular, then we have $a = 0$ and $[(E,G,\alpha)] \in C_0(k)$. If E is ordinary, we also have $[(E,G,\alpha)] \in C_a(k)$. Thus, we have $Y_{0,*}(N,r)_{\mathbf{F}_p} = \bigcup_{a=0}^{e} C_a$. If E is supersingular, we have $G = \operatorname{Ker} F^e$ and $[(E,G,\alpha)] \in C_a(k)$ for all $0 \leq a \leq e$. Thus, the mapping $j_a : Y(r)_{\mathbf{F}_p}^{\mathrm{ss}} \to Y_{0,*}(N,r)_{\mathbf{F}_p}^{\mathrm{ss}}$ is a bijection.

By Lemma 8.4, C_0^{ord} equals the open subscheme of $Y_{0,*}(N,r)_{\mathbf{F}_p}$ defined by the condition that the dual of $E \to E/G$ is étale. Thus, the multiplicity of C_0 equals 1. Similarly, C_e^{ord} equals the open subscheme of $Y_{0,*}(N,r)_{\mathbf{F}_p}$ defined by the condition that G is étale, and thus its multiplicity equals 1.

(3) Let (E,G,α) be an elliptic curve with universal level structure over the intersection $C_a \cap C_{a'}$. Let $b = e-a$ and $b' = e-a'$. If $a < a' \leq e/2$, then since we have $G = \operatorname{Ker} p^{a'}F^{b'-a'} = \operatorname{Ker} p^a F^{b-a}$, we have $\operatorname{Ker} p^{a'-a} = \operatorname{Ker} F^{2(a'-a)}$, and thus E is supersingular. The case $e/2 \leq a < a'$ is similar. Suppose $a < e/2 < a'$. Let $E' \to E$ be the dual of $E \to E' = E/G$. The composition $E \to E' \to E$ equals $p^{b'}F^{a'-b'} \circ p^a F^{b-a} = p^e$. Thus, we have $\operatorname{Ker} p^{a'-a} = \operatorname{Ker} F^{2(a'-a)}$, and E is supersingular in this case, too. The case $a' < e/2 < a$ is similar. This concludes the proof that the intersection $C_a \cap C_{a'}$ is a closed subscheme of C_a^{ss}.

We now show $C_a^{\mathrm{ss}} \subset C_a \cap C_{a'}$. Let G be the universal cyclic subgroup scheme over C_a^{ss}. If $a, a' \leq e/2$, then $G = \operatorname{Ker} p^a F^{b-a} = \operatorname{Ker} p^{a'}F^{b'-a'}$, and thus $C_a^{\mathrm{ss}} \subset C_{a'}$. Similarly, if $a, a' \geq e/2$, we also have $C_a^{\mathrm{ss}} \subset C_{a'}$. If $a < e/2 < a'$, then the kernel of the dual of $E \to E' = E/G$ equals $\operatorname{Ker} p^a V^{b-a} = \operatorname{Ker} p^{a'}F^{b'-a'}$, and again we have $C_a^{\mathrm{ss}} \subset C_{a'}$. The case $a' < e/2 < a$ is also similar. □

COROLLARY 8.58. *If $e = 1$, the regular curve $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ is semistable at p. The fiber $Y_{0,*}(N,r)_{\mathbf{F}_p}$ is the union of C_0 and C_1.*

PROOF. It follows easily from Corollary 8.56, Proposition 8.57 and Lemma B.8. □

PROOF OF THEOREM 8.32. We omit the proof of (1)–(3) since they are similar to the proof of Theorem 8.34.

(4) Let $r \geq 3$ be an integer relatively prime to p. As for the action of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ on $Y_{0,*}(Mp,r)_{\mathbf{Z}[\frac{1}{r}]}$, the inertia group at the generic point of each irreducible component of each fiber is $\{\pm 1\}$. Thus, by Corollaries 8.58 and B.11(2), $Y_0(Mp)$ is weakly semistable, and $j_0, j_1 : Y_0(M)_{\mathbf{F}_p} \to Y_0(Mp)_{\mathbf{F}_p}$ are closed immersions. The intersection of the image C_0 of j_0 and that of C_1 of j_1 is $Y_0(M)^{\mathrm{ss}}_{\mathbf{F}_p} = Y_{0,*}(M,r)^{\mathrm{ss}}_{\mathbf{F}_p}/\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$.

Let $x = [(E,C)] \in Y_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$ be an ordinary double point of $Y_0(Mp)_{\mathbf{F}_p}$, let $x' = [(E,C,\alpha)] \in Y_{0,*}(M,r)^{\mathrm{ss}}_{\mathbf{F}_p}$ be a point in the inverse image of x, and let $\eta = [(E_0,C_0,\alpha_0)]$ be the generic point of

$Y_{0,*}(N,r)_{\mathbf{Z}}$. Then, the inertia group $I_{x'}$ is the image of the injection $\mathrm{Aut}(E_{\overline{\mathbf{F}}_p}, C_{\overline{\mathbf{F}}_p}) \to \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$, and by Lemma 8.41, the inertia group I_η is $\{\pm 1\} \subset \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. Thus, by Corollary B.11(2), the index of x equals $[I_{x'} : I_\eta] = \sharp\,\mathrm{Aut}(E_{\overline{\mathbf{F}}_p}, C_{\overline{\mathbf{F}}_p})/\{\pm 1\}$. □

We define morphisms between modular curves.

PROPOSITION 8.59. *Let S be a scheme, and let E be an elliptic curve over S. Let $N = MdM' \geq 1$ be an integer.*

(1) *Let P be a section of E of exact order N. Then, $P'' = (N/d)P$ has exact order d. Let $H = \sum_{i=0}^{d-1}[iP'']$. Then the image P' of $M'P$ in $E' = E/H$ is a section of exact order M.*
(2) *Let C be a cyclic subgroup scheme of E of order N. Then, there exists a unique cyclic subgroup scheme H of E of order d such that flat locally on S, N/d times of a generator of C is a generator. Moreover, there exists a unique cyclic subgroup scheme C' of $E' = E/H$ of order M such that flat locally on S, M' times of a generator of C is a generator.*

PROOF. (1) It suffices to show the following case: $r \geq 3$ is an integer relatively prime to N, $S = Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$, E is the universal elliptic curve over S, and P is the universal section of exact order N. The assertion is clear on $S[\frac{1}{N}]$. Thus, it suffices to apply Corollary A.44(2) to the closed subscheme $M_1(d)_E$ of E and the section P'', and the closed subscheme $M_1(d)_{E'}$ of E' and the section P'.

(2) Let $X = C^\times$, $S' = M_0(d)_E$, and let H be the universal cyclic subgroup scheme of $E_{S'}$ of order d. By (1), we obtain a morphism $f : X \to Y$ defined by $P \mapsto \langle M'P \rangle \subset E_X/\left(\sum_{i=0}^{d-1}[i\frac{N}{d}P]\right)$. It suffices to show that there exists a section $g : S \to Y$ such that $f : X \to Y$ is the composition of $h : X \to S$ and $g : S \to Y$. Since $h : X \to S$ is faithfully flat, $g : S \to Y$ is unique if it exists.

We show the existence. Let $r \geq 3$ be an integer relatively prime to N. Since the assertion is flat local on S, we may assume there exists a basis α for $E[r]$. Then, (E, C, α) defines a morphism $S \to Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. Thus, it suffices to show the case $S = Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. On $S_{\mathbf{Z}[\frac{1}{N}]}$ the assertion is clear. It now suffices to apply Lemma A.45. □

We define a morphism of functors

$$s_d : \mathcal{M}_1(N) \longrightarrow \mathcal{M}_1(M) \tag{8.52}$$

by sending the isomorphism class of (E, P) to the isomorphism class (E', P'). Similarly, we define a morphism of functors

$$s_d : \mathcal{M}_0(N) \longrightarrow \mathcal{M}_0(M) \tag{8.53}$$

by sending the isomorphism class of (E, C) to the isomorphism class (E', C').

LEMMA 8.60. *Let* $Md \mid N \geq 1$ *be integers. The morphisms of modular curves defined by the morphism of functors* s_d

$$\begin{aligned} s_d &: Y_1(N)_{\mathbf{Z}} \longrightarrow Y_1(M)_{\mathbf{Z}}, \\ s_d &: Y_0(N)_{\mathbf{Z}} \longrightarrow Y_0(M)_{\mathbf{Z}} \end{aligned} \tag{8.54}$$

are finite.

PROOF. We show the morphism $s_d : Y_1(N)_{\mathbf{Z}} \to Y_1(M)_{\mathbf{Z}}$ is finite. Let $r \geq 3$ be an integer relatively prime to N. Define $s_d : Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_{1,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$ in the same way as $s_d : Y_1(N)_{\mathbf{Z}} \to Y_1(M)_{\mathbf{Z}}$. We show this morphism is finite. Let (E, P, α) be the universal elliptic curve with level structure over $S = Y_{1,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$. Let $A = M_0(d)_E$, and let $G \subset E_A$ be the universal cyclic subgroup scheme over A of order d. Let $E' = E_A/G$, and let $g : E' \to E_A$ be the dual of $E_A \to E' = E_A/G$. Let $B = M_1(N)_{E'}$, and let $P' : B \to E'_B$ be the universal section of exact order N. The condition that $g(\frac{N}{Md}P') = P$ and $\frac{N}{d}P'$ is a generator of the kernel of $g : E'_B \to E_B$ is a closed condition on B. Let C be the closed subscheme defined by this closed condition. C is finite over S by Proposition 8.54 and Corollary 8.24. Let $\alpha'_C : (\mathbf{Z}/r\mathbf{Z})^2 \to E'_C[r]$ be the composition of α and the inverse of the isomorphism $E'_C[r] \to E_C[r]$. Then, the triple $(E'_C, P'_C, \alpha'(X))$ defines a morphism $C \to Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$.

We show that the morphism $C \to Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ is an isomorphism and that the composition of the inverse of this and the natural morphism $C \to Y_{1,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$ is $s_d : Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_{1,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$. Let (E', P', α') be the universal elliptic curve over $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ with level structure. The dual $E \to E'$ of $g : E' \to E = E'/\langle \frac{N}{d}P' \rangle$ defines a morphism $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to A$ that extends s_d. The universal section P' defines $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to C \subset B$. It is easy to see that this is the inverse. Thus, $s_d : Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_{1,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$ is finite. Letting $r \geq 3$ run integers relatively prime to N, we obtain a finite morphism $s_d : Y_1(N)_{\mathbf{Z}} \to Y_1(M)_{\mathbf{Z}}$ by taking the quotients and patching them.

Similarly, $s_d : Y_0(N)_{\mathbf{Z}} \to Y_0(M)_{\mathbf{Z}}$ is finite. □

EXAMPLE 8.61. Since $Y_0(4)_{\mathbf{Z}}$ is the quotient of $Y_1(4)_{\mathbf{Z}}$ by the diamond operator $(\mathbf{Z}/4\mathbf{Z})^\times = \{\langle \pm 1\rangle\}$, we have $Y_0(4)_{\mathbf{Z}} = Y_1(4)_{\mathbf{Z}}$. We show

$$Y_1(4)_{\mathbf{Z}} = Y_0(4)_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[s,t,u]/(st-2^8, u(s+2^4)-2^4t, u(t+2^4)-t^2).$$

By the Remark after Theorem 8.34, $Y_1(4)_{\mathbf{Z}}$ is the integral closure of $Y(1)_{\mathbf{Z}} = \operatorname{Spec} \mathbf{Z}[j]$ in $Y_1(4)_{\mathbf{Z}[\frac{1}{4}]}$. Let

$$A = \mathbf{Z}[s,t,u]/(st-2^8, u(s+2^4)-2^4t, u(t+2^4)-t^2).$$

We have $A[\frac{1}{2}] = \mathbf{Z}[\frac{1}{2}][s, \frac{1}{s(s+2^4)}]$. This is isomorphic to $\mathbf{Z}[\frac{1}{4}, d, \frac{1}{d(d-4)}]$ by $s \mapsto 4(d-4)$. Through this isomorphism we identify $Y_1(4)_{\mathbf{Z}[\frac{1}{4}]} = \operatorname{Spec} A[\frac{1}{2}]$.

We show A is an integrally closed domain. $A[\frac{1}{2}] = \mathbf{Z}[\frac{1}{2}][s, \frac{1}{s(s+2^4)}]$ is an integrally closed domain. $A/2A = \mathbf{F}_2[s,t,u]/(st, us, (u-t)t) = \mathbf{F}_2[s,t,u-t]/(st, (u-t)s, (u-t)t)$ is isomorphic to the subring of $\mathbf{F}_2[t] \times \mathbf{F}_2[u] \times \mathbf{F}_2[s]$ given by $\{(f,g,h) \in \mathbf{F}_2[t] \times \mathbf{F}_2[u] \times \mathbf{F}_2[s] \mid f(0) = g(0) = h(0)\}$ by the mapping $s \mapsto (0,0,s), t \mapsto (t,0,0), u \mapsto (t,u,0)$. Thus, $A/2A$ is reduced. $\operatorname{Spec} A$ is smooth over $\mathbf{Z}$ except at the maximal ideal $\mathfrak{m} = (2,s,t,u)$. Thus, by Lemma A.41, A is an integrally closed domain.

If we let $k = s(s+2^4) = 2^4 d(d-4)$, we have $ku = 2^{12}$. By (8.26), the morphism $j : Y_1(4)_{\mathbf{Z}[\frac{1}{4}]} \to Y(1)_{\mathbf{Z}}$ defined by the j-invariant is defined by

$$\begin{array}{cccccc} \mathbf{Z}[j] & \to & A[\frac{1}{2}] & & \supset & A \\ j & \mapsto & 2^8 \cdot \frac{(d^2-4d+1)^3}{d(d-4)} & = \frac{(k+2^4)^3}{k} & = & k^2 + 3 \cdot 2^4 k + 3 \cdot 2^8 + u. \end{array}$$

We show that the integral closure of $\mathbf{Z}[j]$ in $A[\frac{1}{2}]$ is A. Since A is integrally closed, it suffices to show that the generators s, t, u and k are integral over $\mathbf{Z}[j]$. Since we have $s(s+2^4) = k$ and $(k+2^4)^3 = jk$, k and s are integral over $\mathbf{Z}[j]$. Moreover, since $u = j - (k^2 + 3 \cdot 2^4 k + 3 \cdot 2^8)$ and $t^2 = u(t+2^4)$, u and t are also integral over $\mathbf{Z}[j]$. This concludes the proof of $Y_1(4)_{\mathbf{Z}} = \operatorname{Spec} A$.

The intermediate covering $Y_1(2)_{\mathbf{Z}}$ equals $\operatorname{Spec} \mathbf{Z}[k,u]/(ku - 2^{12})$. The surjective morphisms of rings $A/2A \to \mathbf{F}_2[t]$, $A/2A \to \mathbf{F}_2[u]$ and $A/2A \to \mathbf{F}_2[s]$ define closed subschemes C_0, C_1 and $C_2 \subset Y_0(4)_{\mathbf{F}_2}$, respectively. We define isomorphisms $j_i : Y(1)_{\mathbf{F}_2} \to C_i$ $(i = 0,1,2)$ by $t \mapsto j$, $u \mapsto j$ and $s \mapsto j$.

The Atkin–Lehner involution $w_4 : Y_0(4)_{\mathbf{Z}} \to Y_0(4)_{\mathbf{Z}}$ is defined by $s \mapsto t, t \mapsto s, u \mapsto v = s + t - u - 2^4$. It suffices show that

$w_4 : Y_0(4)_{\mathbf{Z}[\frac{1}{4}]} \to Y_0(4)_{\mathbf{Z}[\frac{1}{4}]}$ is defined by $d \mapsto \frac{4d}{d-4}$. Extending the coefficients to $\mathbf{Z}[\sqrt{-1}, \frac{1}{4}]$, we compute $w_4 : Y_1(4)_{\mathbf{Z}[\sqrt{-1},\frac{1}{4}]} \to Y_1(4)_{\mathbf{Z}[\sqrt{-1},\frac{1}{4}]}$. Let $P = (1,1) \in E$ be the universal section of order 4. The quotient $E' = E/\langle 2P\rangle$ of the universal elliptic curve $E : dy^2 = x(x^2 + (d-2)x + 1)$ is given by $dy'^2 = x'(x'+d)(x'+4)$, and $E \to E'$ is given by $x' = x + \frac{1}{x} - 2$, $y' = \frac{y}{x}(x - \frac{1}{x})$. Moreover, $E'' = E/\langle P\rangle$ is given by $dy''^2 = x''(x''^2 - 2(d+4)x'' + (d-4)^2)$. $E' \to E''$ is given by $x'' = x' + d + 4 + \frac{4d}{x'}$, $y'' = \frac{y'}{x'}\left(x' - \frac{4d}{x'}\right)$. If we let $x'' = -(d-4)x_1$ and $y'' = (d-4)^2 2\sqrt{-1}y_1$, E'' is given by $\frac{4d}{d-4}y_1^2 = x_1\left(x_1^2 + \frac{2(d+4)}{d-4}x_1 + 1\right)$. Since the universal section of E'' is given by $(1,1)$, we have $w_4^*(d) = \frac{4d}{d-4}$.

If we let $l = t(t+2^4)$ and $v = s+t-u-2^4$, $s_4 = s_0 \circ w_4 : Y_0(4)_{\mathbf{Z}} \to Y(1)_{\mathbf{Z}}$ is defined by $j \mapsto l^2 + 3\cdot 2^4 l + 3 \cdot 2^8 + v$. Since the j-invariant of E' is $j(E') = 2^4\frac{(d^2-4d+16)^3}{d^2(d-4)^2} = \frac{(k+2^8)^3}{k^2} = k + 3\cdot 2^8 + 3\cdot 2^4 u + u^2$, $s_2 : Y_0(4)_{\mathbf{Z}} \to Y(1)_{\mathbf{Z}}$ is defined by $j \mapsto k + 3\cdot 2^8 + 3\cdot 2^4 u + u^2$. The image of $j = s_1^*j$, s_2^*j, s_4^*j in $\mathbf{F}_2[t]\times\mathbf{F}_2[u]\times\mathbf{F}_2[s]$ is given by (t, u, s^4), (t^2, u^2, s^2), (t^4, u, s), respectively.

8.9. Compactifications

In this book we define the compactification $X_0(N)_{\mathbf{Z}}$ and $X_1(N)_{\mathbf{Z}}$ of modular curves $Y_0(N)_{\mathbf{Z}}$ and $Y_1(N)_{\mathbf{Z}}$ as the integral closure of the j-line. The meaning of these curves as moduli schemes has been studied, but we do not mention it here.

DEFINITION 8.62. Let $N \geq 1$ be an integer.

(1) Define $X_0(N)_{\mathbf{Z}}$ as the integral closure of $\mathbf{P}^1_{\mathbf{Z}}$ with respect to $j : Y_0(N)_{\mathbf{Z}} \to \mathbf{A}^1_{\mathbf{Z}}$.
(2) Define $X_1(N)_{\mathbf{Z}}$ as the integral closure of $\mathbf{P}^1_{\mathbf{Z}}$ with respect to $j : Y_1(N)_{\mathbf{Z}} \to \mathbf{A}^1_{\mathbf{Z}}$.

In this section we prove the following fundamental properties of $X_0(N)_{\mathbf{Z}}$ and $X_1(N)_{\mathbf{Z}}$.

THEOREM 8.63. *Let $N \geq 1$ be an integer.*

(1) *$X_0(N)_{\mathbf{Z}}$ is a normal projective curve over $\mathbf{Z}$, and its each geometric fiber is connected.*
(2) *Let $p \nmid N$ be a prime number. Then, $X_0(N)_{\mathbf{Z}}$ is smooth at p. The fiber $X_0(N)_{\mathbf{F}_p} = X_0(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p$ is a smooth compactification of $Y_0(N)_{\mathbf{F}_p}$.*

(3) *Let $N = Mp$ with $p \nmid M$. Then, $X_0(N)_{\mathbf{Z}}$ is weakly semistable at p. The closed immersions $j_0 : Y_0(M)_{\mathbf{F}_p} \to Y_0(N)_{\mathbf{F}_p}$ and $j_1 : Y_0(M)_{\mathbf{F}_p} \to Y_0(N)_{\mathbf{F}_p}$ extend to closed immersions $j_0 : X_0(M)_{\mathbf{F}_p} \to X_0(N)_{\mathbf{F}_p}$ and $j_1 : X_0(M)_{\mathbf{F}_p} \to X_0(N)_{\mathbf{F}_p}$. The fiber $X_0(N)_{\mathbf{F}_p}$ is the union of the image $\overline{C}_0$ of j_0 and the image $\overline{C}_1$ of j_1, and the intersection of $\overline{C}_0$ and $\overline{C}_1$ is the coarse moduli scheme $Y_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$ of $\mathcal{M}_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$. The index of the ordinary double point $x = [(E,C)] \in Y_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$ is the order of* $\mathrm{Aut}(E_{\bar{\mathbf{F}}_p}, C_{\bar{\mathbf{F}}_p})/\{\pm 1\}$.

Using Theorem 8.63, we compute the number of isomorphism classes of supersingular elliptic curves, which is equal to $\deg Y(1)^{\mathrm{ss}}_{\mathbf{F}_p}$.

COROLLARY 8.64. *Let p be a prime number. Then, we have $Y(1)^{\mathrm{ss}}_{\mathbf{F}_p} \neq \varnothing$. The number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbf{F}}_p$ equals* $\deg Y(1)^{\mathrm{ss}}_{\mathbf{F}_p}$, *which equals*

$$1 + g_0(p) = 1 + \frac{p-a}{12} \quad (\textit{if } p \equiv a = 2, 3, 5, 7, -1, 13 \bmod 12).$$

PROOF. By Theorem 8.63, $X_0(p)_{\mathbf{F}_p} = \overline{C}_0 \cup \overline{C}_1$ is connected. Thus, $\overline{C}_0 \cap \overline{C}_1 = Y(1)^{\mathrm{ss}}_{\mathbf{F}_p}$ is nonempty. Since the coarse moduli scheme $Y(1)^{\mathrm{ss}}_{\mathbf{F}_p}$ is reduced, we have $\deg Y(1)^{\mathrm{ss}}_{\mathbf{F}_p} = \sharp Y(1)^{\mathrm{ss}}_{\mathbf{F}_p}(\overline{\mathbf{F}}_p)$.

We have {isomorphism classes of supersingular elliptic curves over $\overline{\mathbf{F}}_p\} = \mathcal{M}(1)^{\mathrm{ss}}_{\mathbf{F}_p}(\overline{\mathbf{F}}_p) = Y(1)^{\mathrm{ss}}_{\mathbf{F}_p}(\bar{\mathbf{F}}_p)$. By Corollary D.21(1) and the fact that $g_0(1) = 0$, we have $g_0(p) = \deg Y(1)^{\mathrm{ss}}_{\mathbf{F}_p} - 1$. By Proposition 2.15 and Lemma 2.14, we have

$$\begin{aligned} g_0(p) = 1 + \frac{1}{12}(p+1) - \frac{1}{2}\cdot 2 \\ - \frac{1}{3}\begin{cases} 0 & (p \equiv 2 \bmod 3) \\ 1 & (p = 3) \\ 2 & (p \equiv 1 \bmod 3) \end{cases} - \frac{1}{4}\begin{cases} 0 & (p \equiv 3 \bmod 4) \\ 1 & (p = 2) \\ 2 & (p \equiv 1 \bmod 4). \end{cases} \end{aligned} \qquad \square$$

EXAMPLE 8.65. By Example 8.6, the elliptic curves E over $\mathbf{F}_p$ whose j-invariant equals 1728 is supersingular if $p \equiv -1 \bmod 4$, and the elliptic curves E over $\mathbf{F}_p$ whose j-invariant equals 0 is supersingular if $p \equiv -1 \bmod 3$. Thus, by Lemma 8.41 and Corollary 8.64, we obtain

$$\sum_{\substack{\text{isomorphism classes of} \\ \text{supersingular elliptic curves } E}} \frac{1}{\sharp \operatorname{Aut} E} = \frac{p-1}{24}.$$

For a prime number p, the number of supersingular elliptic curves over $\overline{\mathbf{F}}_p$ and their j-invariants are as follows.

p	2	3	5	7	11	13	17	19	$\cdots$
$\sharp$ of s.s. curves[a]	1	1	1	1	2	1	2	2	$\cdots$
s.s. j-invariant[b]	0	0	0	-1	0, 1	6	0, 8	-1, 7	$\cdots$
index[c]	12	6	3	2	3, 2	1	3, 1	2, 1	$\cdots$

[a] number of isomorphism classes of supersingular elliptic curves
[b] j-invariant of supersingular elliptic curve
[c] index at each point $= \frac{1}{2}\sharp\,\mathrm{Aut}(E)$

THEOREM 8.66. *Let $N \geq 1$ be an integer.*

1. *$X_1(N)_{\mathbf{Z}}$ is a normal projective curve over $\mathbf{Z}$ and each geometric fiber is connected.*
2. *Let $p \nmid N$. Then, $X_1(N)_{\mathbf{Z}}$ is smooth at p. The fiber $X_1(N)_{\mathbf{F}_p} = X_1(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{F}_p$ is a smooth compactification of $Y_1(N)_{\mathbf{F}_p}$.*

In order to describe the compactification, we define the Tate curves. In Chapter 2, (2.34), we defined the power series

$$E_k(q) = 1 + \frac{2}{\zeta(1-k)} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in \mathbf{Q}[[q]],$$

where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$. We then defined an elliptic curve over the field of power series $\mathbf{Q}((q))$ by

$$y^2 = 4x^3 - \frac{1}{12}E_4(q)x + \frac{1}{216}E_6(q). \tag{2.35}$$

By the change of coordinates $x = x' + \frac{1}{12}$, $y = 2y' + x'$, the equation (2.35) becomes

$$\begin{aligned} y'^2 + x'y' = x'^3 &- \frac{1}{48}(E_4(q) - 1)x' \\ &- \frac{1}{4\cdot 12^2}(E_4(q) - 1) + \frac{1}{4\cdot 216}(E_6(q) - 1). \end{aligned} \tag{8.55}$$

Let $s_k(q) = \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n = \frac{\zeta(1-k)}{2}(E_k(q) - 1) \in \mathbf{Z}[[q]]$. Since $\zeta(-3) = \frac{1}{120}$ and $\zeta(-5) = -\frac{1}{252}$, the coefficient of the degree 1 term of the right-hand side of (8.55) equals $-5s_4(q)$, and the constant term is $-\frac{1}{12}(5s_4(q) + 7s_6(q))$.

QUESTION. Verify that $\frac{1}{12}(5s_4(q)+7s_6(q)) \in \mathbf{Z}[[q]]$. Let $\mathbf{Z}((q)) = \mathbf{Z}[[q]][q^{-1}]$. Show that the equation

$$y^2 + xy = x^3 - 5s_4(q)x - \frac{1}{12}(5s_4(q)+7s_6(q)) \tag{8.56}$$

defines an elliptic curve over $\mathbf{Z}((q))$.

DEFINITION 8.67. The elliptic curve E_q over $\mathbf{Z}((q)) = \mathbf{Z}[[q]][q^{-1}]$ defined by (8.56) is called the *Tate curve*.

LEMMA 8.68. *The morphism* $e : \operatorname{Spec}\mathbf{Z}((q)) \to Y(1)_{\mathbf{Z}} = \mathbf{A}^1_{\mathbf{Z}}$ *defined by the Tate curve* E_q *extends uniquely to* $\bar{e} : \operatorname{Spec}\mathbf{Z}[[q]] \to X(1)_{\mathbf{Z}} = \mathbf{P}^1_{\mathbf{Z}}$. *Let* $X(1)_{\mathbf{Z}}|^{\wedge}_{\infty}$ *be the completion of* $X(1)_{\mathbf{Z}} = \mathbf{P}^1_{\mathbf{Z}}$ *along* ∞. *Then* $\bar{e}$ *induces an isomorphism* $\hat{e} : \operatorname{Spec}\mathbf{Z}[[q]] \to X(1)_{\mathbf{Z}}|^{\wedge}_{\infty}$.

PROOF. As we have seen Example 2.37 in Chapter 2, the j-invariant of the Tate curve is

$$j(q) = \frac{E_4(q)^3}{\Delta(q)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots .$$

Since we have $\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \in q\mathbf{Z}[[q]]^\times$ and $E_4(q) \in 1+\mathbf{Z}[[q]] \subset \mathbf{Z}[[q]]^\times$, we have $j(q) \in \frac{1}{q}\cdot\mathbf{Z}[[q]]^\times$. The assertion now follows easily. ☐

The following is a proposition concerning torsion points of the Tate curve, for which we omit the proof.

PROPOSITION 8.69. *Let* $N \geq 1$ *be an integer. The group scheme* $E_q[N]$ *of* N*-torsion points of the Tate curve* E_q *is isomorphic to the pullback of* $T[N]$ (8.14) *by the inclusion* $\mathbf{Z}[q,q^{-1}] \to \mathbf{Z}((q))$ *of rings.*

From now on, we identify $E_q[N]$ and $T[N]$ through the isomorphism in Proposition 8.69.

Let $r \geq 1$ be an integer. Define a ring homomorphism $\mathbf{Z}((q)) \to \mathbf{Z}[\frac{1}{r},\zeta_r]((q_r))$ by $q \mapsto q_r^r$. Let $E_{q_r^r}$ be the pullback of the Tate curve E_q over $\mathbf{Z}[\frac{1}{r},\zeta_r]((q_r))$ by this ring homomorphism. We define an isomorphism $\alpha_r : (\mathbf{Z}/r\mathbf{Z})^2 \to E_{q_r^r}[r] = T[r] \otimes_{\mathbf{Z}[q,q^{-1}]} \mathbf{Z}[\frac{1}{r},\zeta_r]((q_r))$ of group schemes over $\mathbf{Z}[\frac{1}{r},\zeta_r]((q_r))$ by $\alpha_r((1,0)) = (0,\zeta_r)$ and $\alpha_r((0,1)) = (1,q_r)$. The morphism $e_r : \operatorname{Spec}\mathbf{Z}[\frac{1}{r},\zeta_r]((q_r)) \to Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ defined by the pair $(E_{q_r^r},\alpha_r)$ is called the morphism defined by the Tate curve. We have $e_1 = e$.

For $a \in (\mathbf{Z}/r\mathbf{Z})^\times$ and $b \in \mathbf{Z}/r\mathbf{Z}$, let $\sigma_{a,b} = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. Define a subgroup $V(\mathbf{Z}/r\mathbf{Z}) = \{\sigma_{a,b} \mid a \in (\mathbf{Z}/r\mathbf{Z})^\times, b \in \mathbf{Z}/r\mathbf{Z}\} \subset \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$, and define an action of $V(\mathbf{Z}/r\mathbf{Z})$ on $\mathbf{Z}[\frac{1}{r},\zeta_r]((q_r))$ by

$\sigma_{a,b}(\zeta_r) = \zeta_r^a$ and $\sigma_{a,b}(q_r) = \zeta_r^b q_r$. We define an action of $-1 \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ as the trivial action.

COROLLARY 8.70. *Let $r \geq 1$ be an integer. The morphism defined by the Tate curve*

$$e_r : \operatorname{Spec} \mathbf{Z}\left[\zeta_r, \frac{1}{r}\right]((q_r)) \to Y(r)_{\mathbf{Z}[\frac{1}{r}]}$$

is compatible with the action of $V(\mathbf{Z}/r\mathbf{Z}) \cdot \{\pm 1\} \subset \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. The commutative diagram induced by e_r

$$\begin{tikzcd} \coprod_{\sigma \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/V(\mathbf{Z}/r\mathbf{Z})\cdot\{\pm 1\}} \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}]((q_r)) \arrow[r] \arrow[d] & Y(r)_{\mathbf{Z}[\frac{1}{r}]} \arrow[d] \\ \operatorname{Spec} \mathbf{Z}[\frac{1}{r}]((q)) \arrow[r, "e_1"] & Y(1)_{\mathbf{Z}[\frac{1}{r}]} \end{tikzcd} \tag{8.57}$$

is Cartesian.

The morphism $e_r : \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}]((q_r)) \to Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ uniquely extends to $\bar{e}_r : \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]] \to X(r)_{\mathbf{Z}[\frac{1}{r}]}$.

PROOF. It is easy to see that $e_r : \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}]((q_r)) \to Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ is compatible with the action of the subgroup $V(\mathbf{Z}/r\mathbf{Z}) \cdot \{\pm 1\} \subset \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. The morphism defined by the diagram (8.57)

$$\coprod_{\sigma \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/V(\mathbf{Z}/r\mathbf{Z})\cdot\{\pm 1\}} \operatorname{Spec} \mathbf{Z}\left[\zeta_r, \frac{1}{r}\right]((q_r)) \to \operatorname{Spec} \mathbf{Z}\left[\frac{1}{r}\right][[q]] \times_{Y(1)_{\mathbf{Z}[\frac{1}{r}]}} Y(r)_{\mathbf{Z}[\frac{1}{r}]}$$

is, by Corollary 8.40(3), a morphism of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/\{\pm 1\}$-torsors over $\operatorname{Spec} \mathbf{Z}[\frac{1}{r}]((q))$, and thus it is an isomorphism.

The integral closure of $\mathbf{Z}[\frac{1}{r}][[q]]$ in $\mathbf{Z}[\zeta_r, \frac{1}{r}]((q_r))$ is $\mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]]$. Thus, the morphism $e_r : \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}]((q_r)) \to Y(r)_{\mathbf{Z}[\frac{1}{r}]}$ uniquely extends to $\bar{e}_r : \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]] \to X(r)_{\mathbf{Z}[\frac{1}{r}]}$. □

The fibered product $\operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}]((q_r)) \underset{e_r \searrow Y(r)_{\mathbf{Z}[\frac{1}{r}]}}{\times} Y_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ is isomorphic to the spectrum of the ring

$$\prod_{dd'=N} \mathbf{Z}\left[\zeta_r, \frac{1}{r}\right]((q_r)) \otimes_{\mathbf{Z}((q))} \mathbf{Z}[\zeta_{d''}]((q))[T]/(T^{d_1} - \zeta_{d''} q^{d'_1}) \tag{8.58}$$

by Proposition 8.26(1). The integral closure of $\mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]]$ in this ring is calculated as follows.

LEMMA 8.71. *Let $m \geq 1$ and $r \geq 1$ be integers, and let $a, b \geq 1$ be relatively prime integers.*

(1) *If we define a ring homomorphism $\mathbf{Z}[q, q^{-1}] \to \mathbf{Z}[\zeta_r, \frac{1}{r}]((q_r))$ by $q \mapsto q_r^r$, the tensor product*

$$\mathbf{Z}\left[\zeta_r, \frac{1}{r}\right]((q_r)) \otimes_{\mathbf{Z}[q,q^{-1}]} \mathbf{Z}[\zeta_m][q, q^{-1}][T]/(T^a - \zeta_m q^b) \tag{8.59}$$

is isomorphic to

$$\prod_{\substack{g \in \mathrm{Gal}(\mathbf{Q}(\zeta_{m'})/\mathbf{Q}) \\ e \mid d_2 \\ h \in \mathrm{Gal}(\mathbf{Q}(\zeta_{md'})/\mathbf{Q}(\zeta_m))}} \mathbf{Z}\left[\zeta_{mdr/m'd'}, \frac{1}{r}\right]((q_r))[T]/(T^{a'} - \zeta_{md} q_r^{br'}).$$

Here, $m' = (m, r)$, $d = (a, r)$, $d' = (d, r/m')$, and we let $a = a'd, r = r'd$. Moreover, $d = d_1 d_2$, where the prime factors of d_1 are prime factors of m and $(m, d_2) = 1$. For a divisor e of d_2, s is the greatest common divisor of r/m' and $d_1 e$. $\zeta_{md_1}^{1/d_2}$ is an md_1th root of unity satisfying $(\zeta_{md_1}^{1/d_2})^{d_2} = \zeta_{md_1}$.

(2) *Let $n \geq 1$, and let $r \mid mn$. The integral closure of $\mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]]$ in $\mathbf{Z}[\zeta_{mn}, \frac{1}{r}]((q_r))[T]/(T^a - \zeta_m q_r^b)$ is isomorphic to $\mathbf{Z}[\zeta_{mn}, \frac{1}{r}][[S]]$. The homomorphism $\mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]] \to \mathbf{Z}[\zeta_{mn}, \frac{1}{r}][[S]]$ is given by $q_r \mapsto \zeta_m^{-c} S^a$ for some positive integer c relatively prime to a.*

PROOF. (1) Since $\mathbf{Z}[\zeta_r, \frac{1}{r}] \otimes_{\mathbf{Z}} \mathbf{Z}[\zeta_m]$ is the integral closure of $\mathbf{Z}[\frac{1}{r}]$ in $\mathbf{Q}(\zeta_r) \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_m) = \prod_{g \in \mathrm{Gal}(\mathbf{Q}(\zeta_{m'})/\mathbf{Q})} \mathbf{Q}(\zeta_{mr/m'})$, it equals $\prod_{g \in \mathrm{Gal}(\mathbf{Q}(\zeta_{m'})/\mathbf{Q})} \mathbf{Z}[\zeta_{mr/m'}, \frac{1}{r}]$. Thus, the ring (8.59) equals

$$\prod_{g \in \mathrm{Gal}(\mathbf{Q}(\zeta_{m'})/\mathbf{Q})} \mathbf{Z}\left[\zeta_{mr/m'}, \frac{1}{r}\right]((q_r))[T]/(T^a - \zeta_m q_r^{br}).$$

Moreover, we have

$$\begin{aligned} &\mathbf{Z}\left[\zeta_{mr/m'}, \frac{1}{r}\right]((q_r))[T]/(T^a - \zeta_m q_r^{br}) \\ &\qquad = \left(\mathbf{Z}\left[\zeta_{mr/m'}, \frac{1}{r}\right]((q_r))[U]/(U^d - \zeta_m)\right)[T]/(T^{a'} - U q_r^{br'}). \end{aligned}$$

Factorize $d = d_1 d_2$, where prime factors of d_1 are prime factors of m and $(m, d_2) = 1$. Then we have

$$\begin{aligned}
\mathbf{Q}(\zeta_{mr/m'})[U]/(U^d - \zeta_m) &= \mathbf{Q}(\zeta_{mr/m'}) \otimes_{\mathbf{Q}(\zeta_m)} \mathbf{Q}(\zeta_m)[U]/(U^d - \zeta_m) \\
&= \mathbf{Q}(\zeta_{mr/m'}) \otimes_{\mathbf{Q}(\zeta_m)} \mathbf{Q}(\zeta_{md_1})[U]/(U^{d_2} - \zeta_{md_1}) \\
&= \mathbf{Q}(\zeta_{mr/m'}) \otimes_{\mathbf{Q}(\zeta_m)} \prod_{e|d_2} \mathbf{Q}(\zeta_{md_1 e}) \\
&= \prod_{e|d_2} \prod_{h \in \mathrm{Gal}(\mathbf{Q}(\zeta_{ms})/\mathbf{Q}(\zeta_m))} \mathbf{Q}(\zeta_{md_1 er/m's}),
\end{aligned}$$

where s is the greatest common divisor of r/m' and $d_1 e$. Since the ring $\mathbf{Z}[\zeta_{mr/m'}, \frac{1}{r}][U]/(U^d - \zeta_m)$ is the integral closure of $\mathbf{Z}[\frac{1}{r}]$ in $\mathbf{Q}(\zeta_{mr/m'})[U]/(U^d - \zeta_m)$, it equals

$$\prod_{e|d_2} \prod_{h \in \mathrm{Gal}(\mathbf{Q}(\zeta_{ms})/\mathbf{Q}(\zeta_m))} \mathbf{Z}\left[\zeta_{mrd_1 e/m's}, \frac{1}{r}\right].$$

Let $\zeta_{md_1}^{1/d_2}$ be an md_1th root of unity satisfying $(\zeta_{md_1}^{1/d_2})^{d_2} = \zeta_{md_1}$. Then, the (e, h)-component of the image of U is $\zeta_{md_1}^{1/d_2}\zeta_e$. Thus, we have

$$\begin{aligned}
&\mathbf{Z}[\zeta_{mr/m'}, \frac{1}{r}]((q_r))[T]/(T^a - \zeta_m q_r^{br}) \\
&= \prod_{e|d_2} \prod_{h \in \mathrm{Gal}(\mathbf{Q}(\zeta_{md'})/\mathbf{Q}(\zeta_m))} \mathbf{Z}\left[\zeta_{mrd_1 e/m's}, \frac{1}{r}\right]((q_r))[T]/(T^{a'} - \zeta_{md_1}^{1/d_2}\zeta_e q_r^{br'}).
\end{aligned}$$

(2) Take positive integers c, d satisfying $bc - ad = 1$, and define a morphism of $\mathbf{Z}[\zeta_{mn}, \frac{1}{r}]$-algebras $\mathbf{Z}[\zeta_{mn}, \frac{1}{r}]((q_r))[T]/(T^a - \zeta_m q_r^b) \to \mathbf{Z}[\zeta_{mn}, \frac{1}{r}]((S))$ by $q_r \mapsto \zeta_m^{-c} S^a$, $T \mapsto \zeta_m^{-d} S^b$. Then, since the inverse is defined by $S \mapsto T^c q_r^{-d}$, this is an isomorphism. Since $\mathbf{Z}[\zeta_{mn}, \frac{1}{r}][[S]]$ is finitely generated as a $\mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]]$-module, the integral closure of $\mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]]$ is $\mathbf{Z}[\zeta_{mn}, \frac{1}{r}][[S]]$. ☐

The compactifications of $Y_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ and $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ are defined similarly to Definition 8.62.

DEFINITION 8.72. Let $N \geq 1$ be an integer, and let $r \geq 3$ be an integer relatively prime to N.

(1) The scheme $X_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ is defined as the integral closure of $X(1)_{\mathbf{Z}[\frac{1}{r}]}$ with respect to $Y_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to Y(1)_{\mathbf{Z}[\frac{1}{r}]}$.

(2) The scheme $X_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ over $\mathbf{Z}[\frac{1}{r}]$ is defined as the integral closure of $X(1)_{\mathbf{Z}[\frac{1}{r}]}$ with respect to $Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to Y(1)_{\mathbf{Z}[\frac{1}{r}]}$.

If $N = 1$, $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} = X_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is denoted by $X(r)_{\mathbf{Z}[\frac{1}{r}]}$.

PROPOSITION 8.73. *Let $N \geq 1$ be an integer, and let $r \geq 3$ be an integer relatively prime to N.*

1. *The scheme $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is a regular projective curve over $\mathbf{Z}[\frac{1}{r}]$. $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{Nr}]}$ is smooth over $\mathbf{Z}[\frac{1}{Nr}]$. The field of constants of the curve $X_{0,*}(N,r)_{\mathbf{Q}} = X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ over $\mathbf{Q}$ equals $\mathbf{Q}(\zeta_r)$.*
2. *Let $p \nmid r$ be a prime number, and let $N = Mp^e$ with $(p, M) = 1$. For $0 \leq a \leq e$, the closed immersion $j_a : Y_{0,*}(M,r)_{\mathbf{F}_p} \to Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ extends to a closed immersion $j_a : X_{0,*}(M,r)_{\mathbf{F}_p} \to X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. If $\overline{C}_a$ is the image of j_a, we have $\overline{C}_a \cap \overline{C}_{a'} = C_a \cap C_{a'} \subset Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ for $a \neq a$. Moreover, if $e = 1$, $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is semistable at p and the closed fiber $X_{0,*}(N,r)_{\mathbf{F}_p}$ is the union of $\overline{C}_0$ and $\overline{C}_1$.*

PROOF. (1) By Corollary 8.56, $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is regular, and $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{Nr}]}$ is smooth over $\mathbf{Z}[\frac{1}{Nr}]$. Let $X(r)_{\mathbf{Z}[\frac{1}{r}]}|^{\wedge}_{\infty}$ be the completion of $X(r)_{\mathbf{Z}[\frac{1}{r}]}$ along the inverse image of $\infty = \mathbf{P}^1_{\mathbf{Z}} - \mathbf{A}^1_{\mathbf{Z}}$. Then, by Lemma 8.68 and Corollary 8.70, we obtain an isomorphism

$$\coprod_{\sigma \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/V(\mathbf{Z}/r\mathbf{Z})\cdot\{\pm 1\}} \operatorname{Spec} \mathbf{Z}\left[\zeta_r, \frac{1}{r}\right][[q_r]] \to X(r)_{\mathbf{Z}[\frac{1}{r}]}|^{\wedge}_{\infty}. \tag{8.60}$$

Let $i_r : \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}] \to X(r)_{\mathbf{Z}[\frac{1}{r}]}$ be the composition of the closed immersion defined by $q_r \mapsto 0$ and the extension $\bar{e}_r : \operatorname{Spec} \mathbf{Z}[\zeta_r, \frac{1}{r}][[q_r]] \to X(r)_{\mathbf{Z}[\frac{1}{r}]}$. Then i_r is a closed immersion. Let $D_r \subset X(r)_{\mathbf{Z}[\frac{1}{r}]}$ be the image of i_r, and let $D_{N,r} = D_r \times_{X(r)_{\mathbf{Z}[\frac{1}{r}]}} X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. By Lemma 8.71, the scheme $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is regular on a neighborhood of $D_{N,r}$, and smooth over $\mathbf{Z}[\frac{1}{Nr}]$. Moreover, for $\sigma \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$, $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is regular on a neighborhood of $\sigma^*(D_{N,r})$ and is smooth over $\mathbf{Z}[\frac{1}{Nr}]$. By (8.60), we have

$$X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} - Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} = \coprod_{\sigma \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})/V(\mathbf{Z}/r\mathbf{Z})\cdot\{\pm 1\}} \sigma^*(D_{N,r}).$$

Thus, $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is regular everywhere and smooth over $\mathbf{Z}[\frac{1}{Nr}]$. Since the field of constants of $Y_{0,*}(N,r)_{\mathbf{Q}}$ is $\mathbf{Q}(\zeta_r)$, the field of constants of $X_{0,*}(N,r)_{\mathbf{Q}}$ is also $\mathbf{Q}(\zeta_r)$.

(2) By (1), the projective curve $X_{0,*}(M,r)_{\mathbf{F}_p}$ over $\mathbf{F}_p$ is a smooth compactification of $Y_{0,*}(M,r)_{\mathbf{F}_p}$. Define a reduced closed subscheme $\overline{C}_a$ of $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ as the closure of the image C_a of the closed immersion $j_a : Y_{0,*}(M,r)_{\mathbf{F}_p} \to Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ in $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. By the proof of (1), $\overline{C}_a$ is smooth on a neighborhood of the intersection with $g^*(D_{N,r})$ over $\mathbf{F}_p$ for each $g \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. Thus, $\overline{C}_a$ is also a smooth compactification of $Y_{0,*}(M,r)_{\mathbf{F}_p}$ and is isomorphic to $X_{0,*}(M,r)_{\mathbf{F}_p}$. Furthermore, by the proof of (1), the reduced part of $X_{0,*}(N,r)_{\mathbf{F}_p}$ is smooth on a neighborhood of the intersection with the inverse image of $g^*(D_r)$ for each $g \in \mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. Thus, if $a \neq a'$, $\overline{C}_a$ and $\overline{C}_{a'}$ do not intersect each other on a neighborhood of the inverse image of each $g^*(D_r)$. Hence, the intersection $\overline{C}_a \cap \overline{C}_{a'}$ is contained in $Y_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$.

The last assertion in the case of $e = 1$ follows easily from the above and Corollary 8.58. □

PROPOSITION 8.74. *Let $N \geq 1$ be an integer, and let $r \geq 3$ be an integer relatively prime to N.*

(1) *The scheme $X_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is a regular projective curve over $\mathbf{Z}[\frac{1}{r}]$. $X_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{Nr}]}$ is smooth over $\mathbf{Z}[\frac{1}{Nr}]$. The field of constants of the curve $X_{1,*}(N,r)_{\mathbf{Q}} = X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ over $\mathbf{Q}$ equals $\mathbf{Q}(\zeta_r)$.*

(2) *Let $p \nmid r$ be a prime number, and let $N = Mp^e$ with $(p,M) = 1$. For $0 \leq a \leq e$, let $\overline{\mathrm{Ig}}(Mp^a,r)_{\mathbf{F}_p}$ be the smooth compactification of the smooth affine curve $\mathrm{Ig}(Mp^a,r)_{\mathbf{F}_p}$ over $\mathbf{F}_p$. Then, the closed immersion $j_a : \mathrm{Ig}(Mp^a,r)_{\mathbf{F}_p} \to Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ extends to a closed immersion $j_a : \overline{\mathrm{Ig}}(Mp^a,r)_{\mathbf{F}_p} \to X_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. If $a \neq a'$, the intersection of the image $\overline{C}_a$ of j_a and the image $\overline{C}_{a'}$ of $j_{a'}$ is contained in $Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$.*

The proof of Proposition 8.74 is similar to that of Proposition 8.73, and we omit it.

PROOF OF THEOREM 8.63. (1) It is clear from the definition that $X_0(N)_{\mathbf{Z}}$ is a normal projective curve over $\mathbf{Z}$. The geometric fiber $X_0(N)_{\overline{\mathbf{Q}}}$ at the generic point is connected by Theorem 2.10(3). Thus, we have $\Gamma(X_0(N)_{\mathbf{Q}}, \mathcal{O}) = \mathbf{Q}$ and $\Gamma(X_0(N)_{\mathbf{Z}}, \mathcal{O}) = \mathbf{Z}$. Hence, by Theorem A.16, each geometric fiber of $X_0(N)_{\mathbf{Z}}$ is connected.

(2) $X_0(N)_{\mathbf{Z}}$ is obtained by patching together the quotients of $X_{0,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$ by $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. Thus by Propositions 8.73 and B.10(1),

$X_0(N)_{\mathbf{Z}[\frac{1}{N}]}$ is smooth over $\mathbf{Z}[\frac{1}{N}]$. Furthermore if $p \nmid N$, $X_0(N)_{\mathbf{F}_p}$ is a quotient of $X_{0,*}(N,r)_{\mathbf{F}_p}$ and it is a smooth compactification of $Y_0(N)_{\mathbf{F}_p}$.

(3) As in (2), if $N = Mp$ with $p \nmid M$, then $X_0(N)_{\mathbf{Z}}$ is weakly semistable at p by Proposition 8.73 and Corollary B.11(2). Since the closures $\overline{C}_0$, $\overline{C}_1$ of the images C_0, C_1 of the closed immersions $j_0, j_1 : Y_0(M)_{\mathbf{F}_p} \to Y_0(N)_{\mathbf{Z}}$ are regular at the cusps, both are isomorphic to $X_0(M)_{\mathbf{F}_p}$. Thus, the closed immersions j_0 and j_1 extend to closed immersions $j_0, j_1 : X_0(M)_{\mathbf{F}_p} \to X_0(N)_{\mathbf{F}_p}$. The facts $X_0(N)_{\mathbf{F}_p} = \overline{C}_0 \cup \overline{C}_1$ and $\overline{C}_0 \cap \overline{C}_1 = Y_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$ follow easily from Proposition 8.73. □

Since the proof of Theorem 8.66 is similar to above, we omit it. Similarly to Theorem 8.63, we have Theorem 8.76 below.

DEFINITION 8.75. Let $M \geq 1$ and $N \geq 1$ be integers relatively prime to each other.

Define a functor $\mathcal{M}_{1,0}(M,N)$ over $\mathbf{Z}$ by associating to a scheme T the set

$$\mathcal{M}_{1,0}(M,N)(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E,P,C), \\ \text{where } E \text{ is an elliptic curve over } T,\ P \text{ is} \\ \text{a section of } E \text{ of exact order } M, \text{ and } C \text{ is a} \\ \text{cyclic subgroup scheme of order } N \end{array} \right\}.$$

For a prime number $p \mid M$, we define the restrictions of functors $j_0, j_1 : \mathcal{M}_1(M)_{\mathbf{F}_p} \to \mathcal{M}_{1,0}(M,p)_{\mathbf{F}_p}$ by $[(E,P)] \mapsto [(E,P,\operatorname{Ker} F)]$ and $[(E,P)] \mapsto [(E^{(p)}, P^{(p)}, \operatorname{Ker} V)]$.

THEOREM 8.76. *Let $M \geq 1$ and $N \geq 1$ be integers relatively prime to each other.*

(1) *There exists a coarse moduli scheme $Y_{1,0}(M,N)_{\mathbf{Z}}$ of the functor $\mathcal{M}_{1,0}(M,N)$ over $\mathbf{Z}$. $Y_{1,0}(M,N)_{\mathbf{Z}}$ is a normal connected affine curve over $\mathbf{Z}$, and the morphism defined by the j-invariant, $j : Y_{1,0}(M,N)_{\mathbf{Z}} \to \mathbf{A}^1_{\mathbf{Z}}$, is finite flat.*

(2) *Let $N = p$ be a prime number. The integral closure $X_{1,0}(M,p)_{\mathbf{Z}}$ of $\mathbf{P}^1_{\mathbf{Z}}$ with respect to the finite morphism $j : Y_{1,0}(M,p)_{\mathbf{Z}} \to \mathbf{A}^1_{\mathbf{Z}}$ is weakly semistable at p. The restrictions of functors $j_0, j_1 : \mathcal{M}_{1,0}(M)_{\mathbf{F}_p} \to \mathcal{M}_{1,0}(M,p)_{\mathbf{F}_p}$ induce closed immersions $j_0, j_1 : Y_1(M)_{\mathbf{F}_p} \to Y_{1,0}(M,p)_{\mathbf{Z}}$, and they extend to closed immersions $j_0, j_1 : X_1(M)_{\mathbf{F}_p} \to X_{1,0}(M,p)_{\mathbf{Z}}$. $X_{1,0}(M,p)_{\mathbf{F}_p}$ is the union of the image $\overline{C}_0$ of j_0 and the image $\overline{C}_1$ of j_1.*

We omit the proof of this theorem, too.

The integral closure $X_{1,0}(M,N)_{\mathbf{Z}}$ of $\mathbf{P}^1_{\mathbf{Z}}$ with respect to the finite morphism $j : Y_{1,0}(M,N)_{\mathbf{Z}} \to \mathbf{A}^1_{\mathbf{Z}}$ may also be denoted by $X_{0,1}(N,M)_{\mathbf{Z}}$ in this work. $X_{1,0}(M,N)_{\mathbf{Z}}$ is the quotient of $X_1(MN)_{\mathbf{Z}}$ by $(\mathbf{Z}/N\mathbf{Z})^\times \subset (\mathbf{Z}/MN\mathbf{Z})^\times$. The quotient of $X_{1,0}(M,N)_{\mathbf{Z}}$ by $(\mathbf{Z}/M\mathbf{Z})^\times$ identified with $(\mathbf{Z}/MN\mathbf{Z})^\times/(\mathbf{Z}/N\mathbf{Z})^\times$ is $X_0(MN)_{\mathbf{Z}}$. For an integer $r \geq 3$ relatively prime to MN, $X_{1,0,*}(M,N,r)_{\mathbf{Z}[\frac{1}{r}]}$ is also defined similarly.

Unlike Theorem 8.63(3), $X_1(Mp)_{\mathbf{Q}}$, where $p \nmid M$, may not have semistable reduction at p. However, the extension of the base change $X_1(Mp)_{\mathbf{Q}(\zeta_p)} = X_1(Mp)_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_p)$ has semistable reduction at a prime ideal lying above p.

THEOREM 8.77. *Let p be a prime number, let $M \geq 1$ be an integer relatively prime to p, and let $r \geq 3$ be an integer relatively prime to Mp. Let $X_{1,*}(Mp,r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r},\zeta_p]}$ be the normalization of the scheme $X_{1,*}(Mp,r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Z}[\frac{1}{r},\zeta_p]$. Then, the curve $X_{1,*}(Mp,r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r},\zeta_p]}$ over $\mathbf{Z}[\frac{1}{r},\zeta_p]$ is semistable at the prime ideal $\mathfrak{p} = (\zeta_p - 1)$. There exists a closed immersion*

$$j_0, j_1 : \overline{\mathrm{Ig}}(Mp,r)_{\mathbf{F}_p} \longrightarrow X_{1,*}(Mp,r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r},\zeta_p]} \tag{8.61}$$

satisfying the following condition. Let C_0, C_1 be the images of j_0, j_1. We have $X_{1,*}(Mp,r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r},\zeta_p]} \otimes_{\mathbf{Z}[\zeta_p]} \mathbf{F}_p = C_0 \cup C_1$ and $C_0 \cap C_1 = C_0^{\mathrm{ss}}$. The diagrams

(8.62)

$$\begin{tikzcd}
\overline{\mathrm{Ig}}(Mp,r)_{\mathbf{F}_p} \arrow[r] \arrow[d, "j_0"'] & X_{1,*}(M,r)_{\mathbf{F}_p} \arrow[r, equal] \arrow[d, "j_0"'] & X_{1,*}(M,r)_{\mathbf{F}_p} \arrow[d, "j_0"] \\
X_{1,*}(Mp,r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r},\zeta_p]} \arrow[r] & X_{1,*}(Mp,r)_{\mathbf{Z}[\frac{1}{r}]} \arrow[r] & X_{1,0,*}(M,p,r)_{\mathbf{Z}[\frac{1}{r}]}
\end{tikzcd}$$

and

$$\begin{tikzcd}
\overline{\mathrm{Ig}}(Mp,r)_{\mathbf{F}_p} \arrow[r, equal] \arrow[d, "j_1"'] & \overline{\mathrm{Ig}}(Mp,r)_{\mathbf{F}_p} \arrow[r] \arrow[d, "j_1"'] & X_{1,*}(M,r)_{\mathbf{Z}[\frac{1}{r}]} \arrow[d, "j_1"] \\
X_{1,*}(Mp,r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r},\zeta_p]} \arrow[r] & X_{1,*}(Mp,r)_{\mathbf{Z}[\frac{1}{r}]} \arrow[r] & X_{1,0,*}(M,p,r)_{\mathbf{Z}[\frac{1}{r}]}
\end{tikzcd}$$

are commutative.

We will not prove this theorem.

Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p. Let $r \geq 3$ be an integer relatively prime to Mp, and let

$a \geq 0$ be an integer. The quotient of the Igusa curve $\overline{\mathrm{Ig}}(Mp^a, r)_{\mathbf{F}_p}$ by $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ is denoted by $\overline{\mathrm{Ig}}(Mp^a)_{\mathbf{F}_p}$. If $a = 0$, then we have $\overline{\mathrm{Ig}}(Mp^a)_{\mathbf{F}_p} = X_1(M)_{\mathbf{F}_p}$.

COROLLARY 8.78. *Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p. Let $X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\zeta_p]}$ be the integral closure of $X_1(Mp)_{\mathbf{Z}}$ in $X_1(Mp)_{\mathbf{Q}(\zeta_p)} = X_1(Mp)_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_p)$. The curve $X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\zeta_p]}$ over $\mathbf{Z}[\zeta_p]$ is weakly semistable at the prime ideal $\mathfrak{p} = (\zeta_p - 1)$. The closed immersion* (8.61) *induces a closed immersion*

$$j_0, j_1 : \overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p} \longrightarrow X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\zeta_p]}. \tag{8.63}$$

Let C_0, C_1 be the images of j_0, j_1. Then we have $X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\zeta_p]} \otimes_{\mathbf{Z}[\zeta_p]} \mathbf{F}_p = C_0 \cup C_1$ and $C_0 \cap C_1 = C_0^{\mathrm{ss}}$. For $i = 0, 1$, the diagram

$$\begin{tikzcd} \overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p} \arrow[r] \arrow[d, "j_i"'] & X_1(M)_{\mathbf{F}_p} \arrow[d, "j_i"] \\ X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\zeta_p]} \arrow[r] & X_{1,0}(M, p)_{\mathbf{Z}} \end{tikzcd} \tag{8.64}$$

is commutative.

PROOF. $X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r}, \zeta_p]}$ is a quotient of $X_{1,*}(Mp, r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r}, \zeta_p]}$ by the action of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$. By Lemma 8.41(2), the inertia group at the generic point of the fiber $X_{1,*}(Mp, r)_{\mathbf{Q}(\zeta_p)}$ over $\mathbf{Q}(\zeta_p)$ is 1 if $Mp > 2$, and $\{\pm 1\}$ if $Mp \leq 2$. Thus, the assertion follows from Theorem 8.77 and Corollary B.11(2). □

The morphisms $s_d : Y_1(N)_{\mathbf{Z}} \to Y_1(M)_{\mathbf{Z}}$ and $s_d : Y_0(N)_{\mathbf{Z}} \to Y_0(M)_{\mathbf{Z}}$, which we defined in Lemma 8.60, uniquely extend to the compactification.

LEMMA 8.79. *Let $N \geq 1$ be an integer, and let $dM \mid N$. The morphisms of modular curves $s_d : Y_1(N)_{\mathbf{Z}} \to Y_1(M)_{\mathbf{Z}}$ and $s_d : Y_0(N)_{\mathbf{Z}} \to Y_0(M)_{\mathbf{Z}}$ extend uniquely to finite morphisms*

$$\begin{aligned} s_d &: X_1(N)_{\mathbf{Z}} \longrightarrow X_1(M)_{\mathbf{Z}}, \\ s_d &: X_0(N)_{\mathbf{Z}} \longrightarrow X_0(M)_{\mathbf{Z}}. \end{aligned} \tag{8.65}$$

OUTLINE OF PROOF. Let $r \geq 3$ be an integer relatively prime to N. Since $s_d : Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]} \to Y_{1,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$ is a morphism of two-dimensional regular schemes, it uniquely extends to a morphism $X' \to X_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$ from the scheme $X' \to X_{1,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$ obtained by blowing up finitely many times at finitely many closed points of

$X_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} - Y_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]}$. We then show that a morphism $s_d : X_{1,*}(N,r)_{\mathbf{Z}[\frac{1}{r}]} \to X_{1,*}(M,r)_{\mathbf{Z}[\frac{1}{r}]}$ is obtained without taking blowups. Dividing these by the action of $\mathrm{GL}_2(\mathbf{Z}/r\mathbf{Z})$ and patching them up, we obtain the morphism $s_d : X_1(N)_{\mathbf{Z}} \to X_1(M)_{\mathbf{Z}}$. A similar proof works for $s_d : X_0(N)_{\mathbf{Z}} \to X_0(M)_{\mathbf{Z}}$. ☐

QUESTION. Complete the proof of Lemma 8.79.

CHAPTER 9

Modular forms and Galois representations

As we announced in Chapter 2, in this chapter we construct Galois representations associated with modular forms. We show that these satisfy the required conditions using Theorems 8.63 and 8.66, which are fundamental properties of modular curves over **Z**, shown in Chapter 8. In addition, we will prove Theorem 3.52 and a part of Theorem 3.55, which concern ramifications and levels of Galois representations associated with modular forms.

In §9.1, we define some fundamental objects such as Hecke algebras with **Z** coefficients, and then we study Galois representations associated with modular forms using properties of modular curves shown in Chapter 8. In §9.2, we show Theorem 9.16 about the construction of Galois representations associated with modular forms. The key fact here is the congruence relation (Lemma 9.18), which is a consequence of Theorem 8.63(3) concerning the semistable reduction of modular curves. In §9.3, we show the relation between the Hecke algebras with **Z** coefficients and modular mod ℓ representations. In §9.4, we prove Theorem 3.52, which is about the ramification of ℓ-adic representations associated with modular forms and the level of modular forms. In §9.5, we study the action of the Hecke algebras on the image of the space of modular forms of lower level. The proof of the statements in this section requires only the modular curves over **C**, and we do not need modular curves over **Z**. In §9.6, we study the reduction mod p of the Jacobian of $X_0(Mp)$, $p \nmid M$. The results here will play a crucial role in the proof of a part of Theorem 3.55 in §9.7.

9.1. Hecke algebras with Z coefficients

Let $N \geq 1$ be an integer. Let $J_0(N)_{\mathbf{Q}}$ be the Jacobian of the curve $X_0(N)_{\mathbf{Q}}$. $J_0(N)_{\mathbf{Q}}$ is an abelian variety over **Q**. In Chapter 2, we defined the space $S(N)$ of modular forms with **Q** coefficients as $\Gamma(X_0(N), \Omega^1)$. From here on, we write it as $S_0(N)$ instead of $S(N)$ in order to distinguish with the spaces of modular forms $S_1(N) \subset S(N)$, which we will define later. By the natural isomorphism (D.16),

$$\Gamma(J_0(N)_{\mathbf{Q}}, \Omega^1_{J_0(N)_{\mathbf{Q}}/\mathbf{Q}}) \longrightarrow \Gamma(X_0(N)_{\mathbf{Q}}, \Omega^1_{X_0(N)_{\mathbf{Q}}/\mathbf{Q}}) = S_0(N), \tag{9.1}$$

we identify as $S_0(N) = \Gamma(J_0(N)_{\mathbf{Q}}, \Omega^1)$.

In Definition 2.31 we defined the Hecke operator $T_n : S_0(N) \to S_0(N)$ for each integer $n \geq 1$. There, we used the finite flat morphisms $s, t : X_0(N, n) \to X_0(N)_{\mathbf{Q}}$ of curves over $\mathbf{Q}$ and defined it as $T_n = s_* \circ t^*$. From now on, we change the notation to denote $s, t : X_0(N, n) \to X_0(N)_{\mathbf{Q}}$ by $s_n, t_n : I_0(N, n) \to X_0(N)_{\mathbf{Q}}$ instead. The curve $I_0(N, n)$ over $\mathbf{Q}$ is the compactification of the coarse moduli scheme of the functor that associates to a scheme T over $\mathbf{Q}$ the set

$$\mathcal{I}_0(N, n)(T) = \left\{ \begin{array}{l} \text{isomorphism classes of triples } (E, C, C_n), \text{ where} \\ E \text{ is an elliptic curve over } T,\ C \text{ a cyclic sub-} \\ \text{group scheme } C \text{ of order } N, \text{ and } C_n \text{ a subgroup} \\ \text{scheme of order } n \text{ such that } C \cap C_n = 0 \end{array} \right\}.$$

The morphisms $s_n, t_n : I_0(N, n) \to X_0(N)_{\mathbf{Q}}$ are defined by sending (E, C, C_n) to (E, C) and $(E/C_n, (C + C_n)/C_n)$, respectively. Define the Hecke operator $T_n : J_0(N)_{\mathbf{Q}} \to J_0(N)_{\mathbf{Q}}$ as the endomorphism $T_n = t_{n*} \circ s_n^*$ of $J(N)_{\mathbf{Q}}$. If C_i $(i \in I)$ are connected components of $I_0(N, n)$, then T_n is the composition

$$J_0(N)_{\mathbf{Q}} = \operatorname{Jac} X_0(N)_{\mathbf{Q}} \xrightarrow{\prod_i (s_n|_{C_i})^*} \prod_{i \in I} \operatorname{Jac} C_i$$
$$\xrightarrow{\prod_i (t_n|_{C_i})_*} \operatorname{Jac} X_0(N)_{\mathbf{Q}} = J_0(N)_{\mathbf{Q}}.$$

By the identification of (9.1), $S_0(N) = \Gamma(J_0(N)_{\mathbf{Q}}, \Omega^1)$, the Hecke operator $T_n : S_0(N) \to S_0(N)$ coincides with the pullback by $T_n : J_0(N)_{\mathbf{Q}} \to J_0(N)_{\mathbf{Q}}$.

DEFINITION 9.1. Let $N \geq 1$ be an integer. Define the *Hecke algebra* $T_0(N)_{\mathbf{Z}}$ as the subring of $\operatorname{End}(J_0(N)_{\mathbf{Q}})$ generated by the Hecke operators T_n, $n = 1, 2, 3, \ldots$, i.e.,

$$T_0(N)_{\mathbf{Z}} = \mathbf{Z}[T_n, n = 1, 2, 3, \ldots] \subset \operatorname{End} J_0(N)_{\mathbf{Q}}. \tag{9.2}$$

The Hecke algebra $T_0(N)_{\mathbf{Z}} \subset \operatorname{End} J_0(N)_{\mathbf{Q}}$ defined above can be identified with a subalgebra of the Hecke algebra $T(N) \subset \operatorname{End} S_0(N)$ as follows.

LEMMA 9.2. *$T_0(N)_{\mathbf{Z}}$ is a commutative algebra and is finitely generated as a $\mathbf{Z}$-module. To $T \in T_0(N)_{\mathbf{Z}} \subset \operatorname{End} J_0(N)_{\mathbf{Q}}$, we associate $T^* \in \operatorname{End}\Gamma(J_0(N)_{\mathbf{Q}}, \Omega^1) = \operatorname{End} S_0(N)$. Then, we obtain an isomorphism of commutative algebras*

$$T_0(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q} = T_0(N)_{\mathbf{Q}} \longrightarrow T(N). \tag{9.3}$$

The isomorphism (9.3) sends the Hecke operator $T_n : J_0(N) \to J_0(N)$ to the Hecke operator $T_n : S_0(N) \to S_0(N)$.

PROOF. Since $\operatorname{End} J_0(N)_{\mathbf{Q}}$ is a finitely generated free $\mathbf{Z}$-module by Proposition A.51(1), so is the submodule $T_0(N)_{\mathbf{Z}}$.

Since the Hecke operator $T_n : S_0(N) \to S_0(N)$ is the pullback T_n^* of the Hecke operator $T_n : J_0(N)_{\mathbf{Q}} \to J_0(N)_{\mathbf{Q}}$, we obtain a surjective homomorphism $T_0(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q} \to T(N)$. By Proposition A.51(3), this is injective. By Proposition 2.32, $T(N)$ is commutative, so is $T_0(N)_{\mathbf{Z}}$. ☐

From now on, we identify $T(N)$ with $T_0(N)_{\mathbf{Q}}$ through (9.3).

COROLLARY 9.3. *Let K be a field of characteristic 0, and let $f \in S_0(N)_K$ be a primary form with K coefficients. The subfield $K_f = \mathbf{Q}(a_n(f), n \geq 1)$ of K is a finite extension of $\mathbf{Q}$, and $a_n(f)$ is an algebraic integer for each integer $n \geq 0$.*

PROOF. Let $\varphi_f : T(N) = T_0(N)_{\mathbf{Q}} \to K$ be the ring homomorphism defined by the primary form f. Since K_f is the image of $\varphi_f : T_0(N)_{\mathbf{Q}} \to K$, it is a finite extension of $\mathbf{Q}$. Since $a_n(f) = \varphi_f(T_n)$ is in the image of $T_0(N)_{\mathbf{Z}}$, it is an algebraic integer. ☐

EXAMPLE 9.4. If $g_0(N) = 0$, then $T_0(N)_{\mathbf{Z}} = 0$. If $g_0(N) = 1$, then $T_0(N)_{\mathbf{Z}} = \mathbf{Z}$. If $f = \sum_{n=1}^{\infty} a_n(f)q^n$ is the unique primary form of level N, then $T_n = a_n(f)$.

The Atkin–Lehner involution $w = w_N : X_0(N)_{\mathbf{Q}} \to X_0(N)_{\mathbf{Q}}$ induces the involution of $J_0(N)_{\mathbf{Q}}$, $w = w_* : J_0(N)_{\mathbf{Q}} \to J_0(N)_{\mathbf{Q}}$.

LEMMA 9.5. *Let $N \geq 1$ and $n \geq 1$ be integers.*

1. *The endomorphism $T_n^* = s_{n*} \circ t_n^*$ of $J_0(N)_{\mathbf{Q}}$ satisfies $w \circ T_n = T_n^* \circ w$.*
2. *If n and N are relatively prime, then we have $T_n^* = T_n$.*

PROOF. (1) Let T be a scheme over $\mathbf{Q}$. For a triple $(E, C, C_n) \in \mathcal{I}_0(N, n)(T)$, let $E' = E/(C + C_n)$. If we let C' be the kernel of the dual of $E/C_n \to E'$ and C'_n be the kernel of the dual of

$E/C \to E'$, then we have $(E', C', C'_n) \in \mathcal{I}_0(N,n)(T)$. Sending (E, C, C_n) to (E', C', C'_n), we obtain a morphism $\tilde{w} : I_0(N,n) \to I_0(N,n)$. We have $\tilde{w}^2 = \mathrm{id}$, and the diagram

$$\begin{tikzcd}
X_0(N)_{\mathbf{Q}} \arrow[d, "w"'] & I_0(N,n) \arrow[l, "s"'] \arrow[r, "t"] \arrow[d, "\tilde{w}"'] & X_0(N)_{\mathbf{Q}} \arrow[d, "w"] \\
X_0(N)_{\mathbf{Q}} & I_0(N,n) \arrow[l, "t"'] \arrow[r, "s"] & X_0(N)_{\mathbf{Q}}
\end{tikzcd}$$

is commutative. The assertion follows easily from this.

(2) Define a morphism $v : I_0(N,n) \to I_0(N,n)$ by sending (E, C, C_n) to $(E/C_n, C + C_n/C_n, E[n]/C_n)$. Then, we have $v^2 = \mathrm{id}$, and the diagram

$$\begin{tikzcd}
X_0(N)_{\mathbf{Q}} \arrow[d, equal] & I_0(N,n) \arrow[l, "s"'] \arrow[r, "t"] \arrow[d, "v"'] & X_0(N)_{\mathbf{Q}} \arrow[d, equal] \\
X_0(N)_{\mathbf{Q}} & I_0(N,n) \arrow[l, "t"'] \arrow[r, "s"] & X_0(N)_{\mathbf{Q}}
\end{tikzcd}$$

is commutative. The assertion follows easily from this. ☐

Let $X_0(N)^{\mathrm{an}}$ be the compact Riemann surface associated with the curve $X_0(N)_{\mathbf{Q}}$, and let $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ be its singular homology group. The complex torus $J_0(N)^{\mathrm{an}}$ defined by the abelian variety $J_0(N)_{\mathbf{Q}}$ can be identified with $\mathrm{Hom}(S_0(N), \mathbf{C})/H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ through the isomorphism (D.9). Define the Hecke operator T_n on $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ by $T_n = t_* \circ s^*$. Through the injective morphism of algebras

$$\mathrm{End}\, J_0(N)_{\mathbf{Q}} \to \mathrm{End}\, H_1(J_0(N)^{\mathrm{an}}, \mathbf{Z}) = \mathrm{End}\, H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}),$$

$H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ is a $T_0(N)_{\mathbf{Z}}$-module.

PROPOSITION 9.6. *$H_1(X_0(N)^{\mathrm{an}}, \mathbf{Q})$ is a free $T_0(N)_{\mathbf{Q}}$-module of rank* 2.

PROOF. By Proposition 2.55, $\mathrm{Hom}(S_0(N)_{\mathbf{Q}}, \mathbf{Q})$ is a free $T_0(N)_{\mathbf{Q}}$-module of rank 1. Thus, $\mathrm{Hom}(S_0(N)_{\mathbf{C}}, \mathbf{C})$ is a free $T_0(N)_{\mathbf{C}}$-module of rank 1 and a free $T_0(N)_{\mathbf{R}}$-module of rank 2. The natural isomorphism (D.8) gives an isomorphism of $T_0(N)_{\mathbf{R}}$-modules

$$H_1(X_0(N)^{\mathrm{an}}, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{R} \to \mathrm{Hom}(S_0(N)_{\mathbf{C}}, \mathbf{C}).$$

Thus, $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{R}$ is a free $T_0(N)_{\mathbf{R}}$-module of rank 2. Since $T_0(N)_{\mathbf{R}}$ is faithfully flat over $T_0(N)_{\mathbf{Q}}$, $H^1(X_0(N)^{\mathrm{an}}, \mathbf{Q})$ is a free $T_0(N)_{\mathbf{Q}}$-module of rank 2. ☐

$H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ is the dual of the singular cohomology group $H^1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$, and thus, by the Poincaré duality, it is naturally isomorphic to $H^1(X_0(N)^{\mathrm{an}}, \mathbf{Z}(1))$. The cup product of cohomology $H^1(X_0(N)^{\mathrm{an}}, \mathbf{Z}(1)) \times H^1(X_0(N)^{\mathrm{an}}, \mathbf{Z}(1)) \to \mathbf{Z}(1)$ is nondegenerate, and it induces a nondegenerate alternating form

$$(\ ,\ ) : H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \times H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \to \mathbf{Z}(1).$$

For $a \in H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$, define $f_a : H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \to \mathbf{Z}(1)$ by $f_a(b) = (a, wb)$. By the Poincaré duality, the mapping

$$H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \longrightarrow \mathrm{Hom}(H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}), \mathbf{Z}(1)) \tag{9.4}$$

that sends a to f_a is an isomorphism of $\mathbf{Z}$-modules. We consider $\mathrm{Hom}(H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}), \mathbf{Z}(1))$ as a $T_0(N)_{\mathbf{Z}}$-module through $Tf(b) = f(Tb)$.

LEMMA 9.7. *The mapping* (9.4) *is an isomorphism of* $T_0(N)_{\mathbf{Z}}$-*modules.*

PROOF. It suffices to show that (9.4) is a morphism of $T_0(N)_{\mathbf{Z}}$-modules. For $a, b \in H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ and $n \geq 1$, we have $(T_n a, wb) = (a, T_n^* wb)$. Thus, by Lemma 9.5(1), we have $(T_n a, wb) = (a, wT_n b)$, and thus (9.4) is a morphism of $T_0(N)_{\mathbf{Z}}$-modules. ☐

COROLLARY 9.8. (1) *The* $T_0(N)_{\mathbf{Q}}$-*module* $\mathrm{Hom}(T_0(N)_{\mathbf{Q}}, \mathbf{Q})$ *is isomorphic to* $T_0(N)_{\mathbf{Q}}$.

(2) *The* $T_0(N)_{\mathbf{Q}}$-*module* $S_0(N)_{\mathbf{Q}}$ *is isomorphic* $T_0(N)_{\mathbf{Q}}$.

PROOF. (1) Since we have $\mathrm{Hom}_{\mathbf{Q}}(H_1(X_0(N)^{\mathrm{an}}, \mathbf{Q}), \mathbf{Q}(1)) = \mathrm{Hom}_{T_0(N)_{\mathbf{Q}}}(H_1(X_0(N)^{\mathrm{an}}, \mathbf{Q}), \mathrm{Hom}_{\mathbf{Q}}(T_0(N)_{\mathbf{Q}}, \mathbf{Q}(1)))$, by Lemma 9.7 and Proposition 9.6, $\mathrm{Hom}(T_0(N)_{\mathbf{Q}}, \mathbf{Q}(1))^2$ is a free $T_0(N)_{\mathbf{Q}}$-module of rank 2. The assertion follows immediately from this.

(2) The $T_0(N)_{\mathbf{Q}}$-module $\mathrm{Hom}_{\mathbf{Q}}(S_0(N)_{\mathbf{Q}}, \mathbf{Q})$ is isomorphic to $T_0(N)_{\mathbf{Q}}$. Thus, by (1), $S_0(N)_{\mathbf{Q}} = \mathrm{Hom}_{\mathbf{Q}}(\mathrm{Hom}_{\mathbf{Q}}(S_0(N)_{\mathbf{Q}}, \mathbf{Q}), \mathbf{Q})$ is isomorphic to $T_0(N)_{\mathbf{Q}}$. ☐

DEFINITION 9.9. Let $N \geq 1$ be an integer. Define a positive definite Hermitian form on the space of modular forms $S_0(N)_{\mathbf{C}}$ by

$$(f, g) = \frac{\sqrt{-1}}{8\pi^2} \int_{X_0(N)(\mathbf{C})} f \wedge \bar{g} \tag{9.5}$$

for $f, g \in S_0(N)_{\mathbf{C}} = \Gamma(X_0(N)_{\mathbf{C}}, \Omega^1)$. (f, g) is called the *Petersson product.*

LEMMA 9.10. *Let $N \geq 1$ be an integer, and let $n \geq 1$ be an integer relatively prime to N. Then, the Hecke operator $T_n : S_0(N)_{\mathbf{C}} \to S_0(N)_{\mathbf{C}}$ is self-adjoint with respect to the Petersson product.*

PROOF. The adjoint operator of T_n is T_n^*. Thus, the assertion follows immediately from Lemma 9.5(2). □

COROLLARY 9.11. *Let $N \geq 1$ be an integer.*

1. *The reduced Hecke algebra with $\mathbf{R}$ coefficients $T_0'(N)_{\mathbf{R}} \subset T_0(N)_{\mathbf{R}}$ generated by T_n with $(n, N) = 1$ is isomorphic to the product ring $\mathbf{R}^{\dim T_0(N)'_{\mathbf{R}}}$.*
2. *The reduced Hecke algebra with $\mathbf{Q}$ coefficients $T_0'(N)_{\mathbf{Q}} \subset T_0(N)_{\mathbf{Q}}$ is generated by T_n with $(n, N) = 1$ is reduced. Let $\Phi_0(N) = \operatorname{Spec} T_0(N)'_{\mathbf{Q}}$, and K_f the residue field for $f \in \Phi_0(N)$. Then, we have $T_0'(N)_{\mathbf{Q}} = \prod_{f \in \Phi_0(N)} K_f$, and each K_f is a totally real field.*
3. *Let $f \in S_0(N)_{\mathbf{C}}$ be a primitive form with complex coefficients. Then, a_n is a real number for all integers $n \geq 1$.*

PROOF. (1) Commutative Hermitian matrices can be diagonalized simultaneously.

(2) Follows immediately from (1).

(3) If f is a primitive form, then by Corollary 2.61, we have $\mathbf{Q}(a_n(f); n \geq 1) = \mathbf{Q}(a_n(f); (n, N) = 1)$. Thus, the assertion follows immediately from (1). □

So far we have treated modular forms defined as differential forms on $X_0(N)_{\mathbf{Q}}$, but modular forms defined as differential forms on $X_1(N)$ also have similar properties. Let $N \geq 1$ be an integer. Let $S_1(N) = \Gamma(X_1(N)_{\mathbf{Q}}, \Omega^1)$. Let $J_1(N)_{\mathbf{Q}}$ be the Jacobian of the curve $X_1(N)_{\mathbf{Q}}$. It is an abelian variety over $\mathbf{Q}$. Through the natural morphism (D.16)

$$\Gamma(J_1(N)_{\mathbf{Q}}, \Omega^1) \longrightarrow \Gamma(X_1(N)_{\mathbf{Q}}, \Omega^1) = S_1(N), \tag{9.6}$$

we identify as $S_1(N) = \Gamma(J_1(N)_{\mathbf{Q}}, \Omega^1)$. All the properties of $S_1(N)$ and $J_1(N)$ we describe below are proved similarly to the properties of $S_0(N)$ and $J_0(N)_{\mathbf{Q}}$. So we omit the proofs.

For each integer $n \geq 1$, the Hecke operator $T_n : J_1(N)_{\mathbf{Q}} \to J_1(N)_{\mathbf{Q}}$ is defined as follows. Let $I_1(N, n)$ be the compactification of the coarse moduli scheme of the functor that associates to a scheme

T over $\mathbf{Q}$ the set

$$\left\{\begin{array}{l}\text{isomorphism classes of triples } (E,P,C)\text{, where } E \text{ is an}\\ \text{elliptic curve over } T,\ P \text{ is a point of } E \text{ of exact order } N,\\ \text{and } C \text{ is a subgroup of degree } n \text{ such that } \langle P\rangle\cap C=0.\end{array}\right\}.$$

$I_1(N,n)$ is a proper smooth curve over $\mathbf{Q}$. To (E,P,C), associating (E,P) and $(E/C,\text{image of }P)$, respectively, we obtain finite flat morphisms $s_n, t_n : I_1(N,n) \to X_1(N)_{\mathbf{Q}}$ of curves over $\mathbf{Q}$. Define an endomorphism T_n by $T_n = t_{n*} \circ s_n^*$. We call it the Hecke operator. We define the Hecke operator $T_n : S_1(N) \to S_1(N)$ as the pullback of $T_n : J_1(N)_{\mathbf{Q}} \to J_1(N)_{\mathbf{Q}}$. For $a \in (\mathbf{Z}/N\mathbf{Z})^\times$, the diamond operator $\langle a\rangle : X_1(N)_{\mathbf{Q}} \to X_1(N)_{\mathbf{Q}}$ induces an automorphism $\langle a\rangle = \langle a\rangle_*$ on $J_1(N)_{\mathbf{Q}}$ and an automorphism $\langle a\rangle = \langle a\rangle^*$ on $S_1(N)$.

The Hecke algebra $T_1(N)_{\mathbf{Z}}$ is defined as the subalgebra

$$T_1(N)_{\mathbf{Z}} = \mathbf{Z}[T_n; n \geq 1, \langle a\rangle; a \in (\mathbf{Z}/N\mathbf{Z})^\times] \tag{9.7}$$

of $\operatorname{End} J_1(N)_{\mathbf{Q}}$. The Hecke algebra $T_1(N)_{\mathbf{Z}}$ is commutative and we have

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p:\text{prime}} \left(1 - T_p p^{-s} + \langle p\rangle p \cdot p^{-2s}\right)^{-1}. \tag{9.8}$$

Here we defined $\langle p\rangle = 0$ for $p \mid N$. By (9.8), we have

$$T_1(N)_{\mathbf{Z}} = \mathbf{Z}[T_p; p : \text{prime}, \langle a\rangle; a \in (\mathbf{Z}/N\mathbf{Z})^\times].$$

$T_1(N)_{\mathbf{Z}}$ is a finitely generated free $\mathbf{Z}$-module.

Define a morphism $w : X_1(N)_{\mathbf{Q}(\zeta_N)} \to X_1(N)_{\mathbf{Q}(\zeta_N)}$ as follows. For an elliptic curve E, let $(\ ,\ )_N : N : E[N] \times E[N] \to \mu_N$ be the Weil pairing. Regard T as a scheme over $\mathbf{Q}(\zeta_N)$. Let $E' = E/\langle P\rangle$ for the pair $(E,P) \in \mathcal{M}_1(N)(T)$, and let P' be the image of $Q \in E[N]$ satisfying $(P,Q)_N = \zeta_N$. Then, we have $(E',P') \in \mathcal{M}_1(N)(T)$. Sending (E,P) to (E',P'), we obtain a morphism $w : X_1(N)_{\mathbf{Q}(\zeta_N)} \to X_1(N)_{\mathbf{Q}(\zeta_N)}$. We have $w^2 = \langle -1\rangle$.

Let $n \geq 1$ be an integer. We define an involution $\tilde{w} : I_1(N,n)_{\mathbf{Q}(\zeta_N)} \to I_1(N,n)_{\mathbf{Q}(\zeta_N)}$ as follows. Let T be a scheme over $\mathbf{Q}(\zeta_N)$. For a triple $(E,P,C) \in \mathcal{I}_1(N,n)(T)$, let $E' = E/(\langle P\rangle + C)$, let $P' \in E'[N]$ be the image of a point Q in E/C satisfying (image of $P, Q) = \zeta_N$, and let C' be the kernel of the dual of $E/C \to E'$. Then, we have $(E',P',C') \in \mathcal{I}_1(N,n)(T)$. Sending (E,P,C) to (E',P',C'), we obtain a morphism $\tilde{w} : I_1(N,n) \to I_1(N,n)$. We have $\tilde{w}^2 = \langle -1\rangle$. The diagram

$$\begin{tikzcd}
X_1(N)_{\mathbf{Q}} \arrow[d, "w"'] & I_1(N,n) \arrow[l, "s"'] \arrow[r, "t"] \arrow[d, "\bar{w}"'] & X_1(N)_{\mathbf{Q}} \arrow[d, "w"] \\
X_1(N)_{\mathbf{Q}} & I_1(N,n) \arrow[l, "t"'] \arrow[r, "s"] & X_1(N)_{\mathbf{Q}}
\end{tikzcd}$$

is commutative. From this we have $w \circ T_n = T_n^* \circ w$.

Let $n \geq 1$ be an integer relatively prime to N. Let $v : I_1(N,n) \to I_1(N,n)$ be the morphism defined by sending a triple (E,P,C) to $(E/C, \text{image of } P, E/C)$. Then, v is an automorphism, and the diagram

$$\begin{tikzcd}
X_1(N)_{\mathbf{Q}} \arrow[d, "\langle n\rangle"'] & I_1(N,n) \arrow[l, "s"'] \arrow[r, "t"] \arrow[d, "v"'] & X_1(N)_{\mathbf{Q}} \arrow[d, equal] \\
X_1(N)_{\mathbf{Q}} & I_1(N,n) \arrow[l, "t"'] \arrow[r, "s"] & X_1(N)_{\mathbf{Q}}
\end{tikzcd}$$

is commutative. Thus, the endomorphism $T_n^* = s_* \circ t^*$ of $J_1(N)_{\mathbf{Q}}$ is equal to $\langle n\rangle \circ T_n$. We have $w \circ \langle a\rangle = \langle a\rangle \circ w$ for $a \in (\mathbf{Z}/N\mathbf{Z})^\times$.

For an integer $n \geq 1$, we define the Hecke operator T_n of the singular homology group $H_1(X_1(N)^{\text{an}}, \mathbf{Z})$ by $T_n = t_* \circ s^*$, and for $a \in (\mathbf{Z}/N\mathbf{Z})^\times$ we define the diamond operator $\langle a\rangle$ by $\langle a\rangle = \langle a\rangle_*$. $H_1(X_1(N)^{\text{an}}, \mathbf{Z})$ is a $T_1(N)_{\mathbf{Z}}$-module, and $H_1(X_1(N)^{\text{an}}, \mathbf{Q})$ is a free $T_1(N)_{\mathbf{Q}}$-module of rank 2. Define an isomorphism of $T_1(N)_{\mathbf{Z}}$-modules

$$H_1(X_1(N)^{\text{an}}, \mathbf{Z}) \longrightarrow \operatorname{Hom}(H_1(X_1(N)^{\text{an}}, \mathbf{Z}), \mathbf{Z}(1)) \tag{9.9}$$

by sending $a \in H_1(X_1(N)^{\text{an}}, \mathbf{Z})$ to the linear form $H_1(X_1(N)^{\text{an}}, \mathbf{Z}) \to \mathbf{Z}(1)$ that send b to (a, wb). The $T_1(N)_{\mathbf{Q}}$-module $\operatorname{Hom}(T_1(N)_{\mathbf{Q}}, \mathbf{Q})$ is isomorphic to $T_1(N)_{\mathbf{Q}}$.

The Petersson product on $S_1(N)_{\mathbf{C}}$ is defined by

$$(f,g) = \frac{\sqrt{-1}}{8\pi^2} \int_{X_1(N)(\mathbf{C})} f \wedge \bar{g} \tag{9.10}$$

for $f, g \in S_1(N)_{\mathbf{C}} = \Gamma(X_1(N)_{\mathbf{C}}, \Omega^1)$. For an integer $n \geq 1$ relatively prime to N, the adjoint operator of the Hecke operator T_n is $\langle n\rangle^{-1} \circ T_n$, and the adjoint of $\langle n\rangle$ is $\langle n\rangle^{-1}$. By the fact that commuting normal matrices can be diagonalized simultaneously, the reduced Hecke algebra with complex coefficients $T_1'(N)_{\mathbf{C}} = \mathbf{C}[T_n, \langle n\rangle; (n,N) = 1] \subset T_1(N)_{\mathbf{C}}$ is isomorphic to the product ring $\mathbf{C}^{\dim T_1'(N)_{\mathbf{C}}}$. The reduced

Hecke algebra with rational coefficients $T_1'(N)_{\mathbf{Q}} = \mathbf{Q}[T_n, \langle n\rangle; (n,N) = 1] \subset T_1(N)_{\mathbf{Q}}$ is isomorphic to the product ring of a finite number of number fields.

The relation between $S_1(N)$ and $S_0(N)$ and that between $T_1(N)$ and $T_0(N)$ are as follows. The natural morphism $X_1(N)_{\mathbf{Q}} \to X_0(N)_{\mathbf{Q}}$ that sends (E,P) to $(E,\langle P\rangle)$ induces a surjective morphism of Jacobians $J_1(N)_{\mathbf{Q}} \to J_0(N)_{\mathbf{Q}}$. The pullback by this morphism defines a natural injective morphism $S_0(N) \to S_1(N)$. Since $X_0(N)_{\mathbf{Q}}$ is the quotient of $X_1(N)_{\mathbf{Q}}$ by the action of the diamond operators $(\mathbf{Z}/N\mathbf{Z})^\times$, we identify $S_0(N)$ with the invariant part $S_1(N)^{(\mathbf{Z}/N\mathbf{Z})^\times}$ through the natural injection $S_0(N) \to S_1(N)$. For an integer $n \geq 1$, the diagram

$$\begin{tikzcd}
X_1(N)_{\mathbf{Q}} \arrow[d] & I_1(N,n) \arrow[l, "s_n"'] \arrow[r, "t_n"] \arrow[d] & X_1(N)_{\mathbf{Q}} \arrow[d] \\
X_0(N)_{\mathbf{Q}} & I_0(N,n) \arrow[l, "s_n"'] \arrow[r, "t_n"] & X_0(N)_{\mathbf{Q}}
\end{tikzcd}$$

is commutative. Moreover, the two squares induce isomorphisms $I_1(N,n) \to$ (the normalization of $I_0(N,n) \times_{X_0(N)_{\mathbf{Q}}} X_1(N)_{\mathbf{Q}})$), the natural surjection $J_1(N)_{\mathbf{Q}} \to J_0(N)_{\mathbf{Q}}$ is compatible with the Hecke operator T_n. Thus, we define a ring homomorphism $T_1(N)_{\mathbf{Z}} \to T_0(N)_{\mathbf{Z}}$ by sending T_n to T_n for any integer $n \geq 1$ and $\langle a\rangle$ to 1. The natural surjection $J_1(N)_{\mathbf{Q}} \to J_0(N)_{\mathbf{Q}}$ and the natural injection $S_0(N) \to S_1(N)$ are compatible with $T_1(N)_{\mathbf{Z}} \to T_0(N)_{\mathbf{Z}}$.

By Proposition 8.69, the pair (E_q, P) of the Tate curve E_q and its point $P = (0, \zeta_N)$ of order N defines a morphism $e : \operatorname{Spec} \mathbf{Q}(\zeta_N)[[q]] \to X_1(N)_{\mathbf{Q}}$. For an extension K of $\mathbf{Q}(\zeta_N)$, $e^* : S_1(N)_K \to K[[q]]dq$ is injective. If $e^*f = \sum_{n=1}^\infty a_n(f) q^n \frac{dq}{q}$ for a modular form $f \in S_1(N)_K$, we call the power series $\sum_{n=1}^\infty a_n(f)q^n$ the q-expansion of f. Since the diagram

$$\begin{tikzcd}
\operatorname{Spec} \mathbf{Q}(\zeta_N)[[q]] \arrow[r] \arrow[d] & X_1(N)_{\mathbf{Q}} \arrow[d] \\
\operatorname{Spec} \mathbf{Q}[[q]] \arrow[r] & X_0(N)_{\mathbf{Q}}
\end{tikzcd}$$

is commutative, so is the diagram

$$\begin{tikzcd}
S_0(N)_K \arrow[r] \arrow[d, "\cap"'] & K[[q]] \arrow[d, equal] \\
S_1(N)_K \arrow[r] & K[[q]].
\end{tikzcd}$$

Let K be a field of characteristic 0. A modular form $f \in S_1(N)_K = S_1(N) \otimes_{\mathbf{Q}} K$ is called a *primary form* if f is an eigenvector of all $T \in T_1(N)_{\mathbf{Z}}$ and $a_1(f) = 1 \in K(\zeta_N)$. Define a ring homomorphism $\varphi_f : T_1(N)_{\mathbf{Z}} \to K$ by $Tf = \varphi_f(T)f$, and we obtain a one-to-one correspondence between primary forms with K coefficients and the ring homomorphisms $\varphi_f : T_1(N)_{\mathbf{Z}} \to K$. For a primary form f with K coefficients, each coefficient $a_n(f) = \varphi_f(T_n)$ of the q-expansion is an algebraic integer. The subfield $\mathbf{Q}(a_n(f), n \geq 1)$ of K is a finite extension of $\mathbf{Q}$.

For a primary form $f \in S_1(N)_K$ with K coefficients, the character $\varepsilon = \varepsilon_f : (\mathbf{Z}/N\mathbf{Z})^\times \to K^\times$ defined by $\langle a \rangle f = \varepsilon(a)f$ is called the *character* of f. ε_f is the composition of $\langle \quad \rangle : (\mathbf{Z}/N\mathbf{Z})^\times \to T_1(N)_{\mathbf{Z}}^\times$ and $\varphi_f : T_1(N)_{\mathbf{Z}}^\times \to K^\times$. For an integer $n \geq 1$, we have $\varphi_f(T_n) = a_n(f)$, and for $a \in (\mathbf{Z}/N\mathbf{Z})^\times$, we have $\varphi_f(\langle a \rangle) = \varepsilon_f(a)$.

For relatively prime integers $N, M \geq 1$, the quotient of $X_1(NM)$ by the subgroup $(\mathbf{Z}/N\mathbf{Z})^\times \subset (\mathbf{Z}/NM\mathbf{Z})^\times$ is denoted by $X_{0,1}(N, M)$. Let $J_{0,1}(N, M)$ be the Jacobian of $X_{0,1}(N, M)$, and define the Hecke algebra $T_{0,1}(N, M)_{\mathbf{Z}}$ as the subring $\mathbf{Z}[T_n; n \geq 1, \langle a \rangle; a \in (\mathbf{Z}/M\mathbf{Z})^\times]$ of $\operatorname{End} J_{0,1}(N, M)$ generated by the Hecke operators T_n, $n \geq 1$, and the diamond operators $\langle a \rangle$, $a \in (\mathbf{Z}/M\mathbf{Z})^\times$.

9.2. Congruence relations

In this section we construct Galois representations associated with modular forms. Let $N \geq 1$ be an integer, and let ℓ be a prime number. Let $T_\ell J_0(N) = \varprojlim_n J_0(N)[\ell^n](\bar{\mathbf{Q}})$ be the Tate module of the Jacobian $J_0(N)$, and let $V_\ell J_0(N) = T_\ell J_0(N) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. These naturally possess the action of the absolute Galois group $G_{\mathbf{Q}} = \operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Define the action of $T \in T_0(N)_{\mathbf{Z}} \subset \operatorname{End} J_0(N)$ as T_*. Then, $T_\ell J_0(N)$ and $V_\ell J_0(N)$ become the $T_0(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell = T_0(N)_{\mathbf{Z}_\ell}$-module and $T_0(N)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = T_0(N)_{\mathbf{Q}_\ell}$-module, respectively. The absolute Galois group $G_{\mathbf{Q}}$ acts on $T_\ell J_0(N)$ and $V_\ell J_0(N)$ as an automorphism of $T_0(N)_{\mathbf{Z}_\ell}$-module and $T_0(N)_{\mathbf{Q}_\ell}$-module, respectively, and these define ℓ-adic representations of $G_{\mathbf{Q}}$.

An isomorphism of $T_0(N)_{\mathbf{Z}}$-modules $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \otimes \mathbf{Z}/\ell^n\mathbf{Z} \to J_0(N)[\ell^n]$ is induced by the natural isomorphism of complex tori $S_0(N)_{\mathbf{C}}/H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \to J_0(N)^{\mathrm{an}}$. It induces an isomorphism of $T_0(N)_{\mathbf{Z}_\ell}$-modules $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \otimes \mathbf{Z}_\ell \to T_\ell J_0(N)$ and an isomorphism of $T_0(N)_{\mathbf{Q}_\ell}$-modules $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \otimes \mathbf{Q}_\ell \to V_\ell J_0(N)$.

Similar facts hold for $T_\ell J_1(N)$ and $V_\ell J_1(N)$.

LEMMA 9.12. *Let $N \geq 1$ be an integer, and let ℓ be a prime number.*

(1) *$V_\ell J_0(N)$ is a free $T_0(N)_{\mathbf{Q}_\ell}$-module of rank 2.*
(2) *$V_\ell J_1(N) = T_\ell J_1(N) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$ is a free $T_1(N)_{\mathbf{Q}_\ell}$-module of rank 2.*
(3) *The natural morphism $X_1(N)_{\mathbf{Q}} \to X_0(N)_{\mathbf{Q}}$ induces an isomorphism of $T_0(N)_{\mathbf{Q}_\ell}$-modules*

$$V_\ell J_1(N) \otimes_{T_1(N)_{\mathbf{Q}_\ell}} T_0(N)_{\mathbf{Q}_\ell} \longrightarrow V_\ell J_0(N). \tag{9.11}$$

PROOF. (1) We have an isomorphism of $T_0(N)_{\mathbf{Q}_\ell}$-modules

$$H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \otimes \mathbf{Q}_\ell \to V_\ell J_0(N),$$

and the assertion follows immediately from Proposition 9.6.

(2) Similar to (1).

(3) The mapping (9.11) is a surjective morphism of free modules of rank 2, which ought to be an isomorphism. □

Taking a basis of $V_\ell J_0(N)$ over $T_0(N)_{\mathbf{Q}_\ell}$, we obtain a continuous representation $G_{\mathbf{Q}} \to \mathrm{GL}_2(T_0(N)_{\mathbf{Q}_\ell})$. The same is true for $V_\ell J_1(N)$. In this section we prove the following theorem.

THEOREM 9.13. *Let $N \geq 1$ be an integer, and let ℓ be a prime number. The ℓ-adic representation $V_\ell J_0(N)$ of $G_{\mathbf{Q}}$ is unramified at primes $p \nmid N\ell$. The characteristic polynomial* $\det(1-\varphi_p t : V_\ell J_0(N)) \in T_0(N)_{\mathbf{Q}_\ell}[t]$ *of the Frobenius substitution φ_p is given by*

$$\det(1 - \varphi_p t : V_\ell J_0(N)) = 1 - T_p t + p t^2.$$

COROLLARY 9.14. *Let ℓ be a prime number, and let K be a finite extension of $\mathbf{Q}_\ell$. Let $f \in S_0(N)_K$ be a primary form of level N with K coefficients. Let V_f be the tensor product $V_\ell J_0(N) \otimes_{T_0(N)_{\mathbf{Q}_\ell}} K$ with respect to the ring homomorphism $T_0(N)_{\mathbf{Q}_\ell} \to K$ defined by f. The ℓ-adic representation V_f of $G_{\mathbf{Q}}$ is unramified at primes p not dividing $N\ell$, and we have*

$$\det(1 - \varphi_p t : V_f) = 1 - a_p(f)t + p t^2.$$

Theorem 3.18(1) follows immediately from Corollary 9.14 by taking a lattice in V_f stable under the action of $G_{\mathbf{Q}}$.

EXAMPLE 9.15. Let $f = \sum_{n=1}^{\infty} a_n(f) q^n$ be the unique primitive form of level 11, and let $E = X_0(11)$. If ℓ is a prime number, $T_\ell E$ is the ℓ-adic representation associated with f, and we have

$$\det(1 - \varphi_p t : T_\ell E) = 1 - a_p(f)t + p t^2$$

for all primes $p \neq \ell, 11$. The solution $(5,5)$ to the equation $y^2+y = x^3-x^2-10x-20$ is a point of order 5, and if $p \neq 11$, we have $5 | \sharp E(\mathbf{F}_p)$. Thus, we have $a_p(f) \equiv p+1 \bmod 5$.

By Lemma 9.12(3), Theorem 9.13 is reduced to the following theorem.

THEOREM 9.16. *Let $N \geq 1$ be an integer, and let ℓ be a prime number. The ℓ-adic representation $V_\ell J_1(N)$ of $G_{\mathbf{Q}}$ is unramified at primes p not dividing $N\ell$, and we have*

$$\det(1-\varphi_p t : V_\ell J_1(N)) = 1 - T_p t + p\langle p\rangle t^2. \tag{9.12}$$

COROLLARY 9.17. *Let ℓ be a prime number, and let K be a finite extension of $\mathbf{Q}_\ell$. Let $f \in S_1(N)_K$ be a primary form of level N of character ε with K coefficients. Define the tensor product $V_f = V_\ell J_1(N) \otimes_{T_0(N)_{\mathbf{Q}_\ell}} K$ by the ring homomorphism $T_1(N)_{\mathbf{Q}_\ell} \to K$ corresponding to f. The ℓ-adic representation V_f of $G_{\mathbf{Q}}$ is unramified at primes p not dividing $N\ell$, and we have*

$$\det(1-\varphi_p t : V_f) = 1 - a_p(f)t + \varepsilon(p)pt^2.$$

The character $\det V_f$ of $G_{\mathbf{Q}}$ is the product of the ℓ-adic cyclotomic character and the composition $G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) = (\mathbf{Z}/N\mathbf{Z})^\times \xrightarrow{\varepsilon} K^\times$.

PROOF OF THEOREM 9.16. Let p be a prime number not dividing $N\ell$. By Theorem 8.63(2), $X_1(N)_{\mathbf{Z}}$ has good reduction at p. Thus, by Lemma D.18, $J_1(N)$ has good reduction at p and $V_\ell J_1(N)$ is an ℓ-adic representation good at p.

We show (9.12). We regard $V_\ell J_1(N)_{\mathbf{F}_p}$ as a $T_1(N)_{\mathbf{Q}_\ell}$-module through the injection $\mathrm{End}\, J_1(N) \to \mathrm{End}\, J_1(N)_{\mathbf{F}_p}$ in Lemma D.11(2). The natural isomorphism $V_\ell J_1(N)_{\mathbf{Q}} \to V_\ell J_1(N)_{\mathbf{F}_p}$ in Lemma D.18 is an isomorphism of $T_1(N)_{\mathbf{Q}_\ell}$-modules. Thus, we have

$$\det(1-\varphi_p t : V_\ell J_1(N)_{\mathbf{Q}}) = \det(1-\varphi_p t : V_\ell J_1(N)_{\mathbf{F}_p}).$$

If $F : J_1(N)_{\mathbf{F}_p} \to J_1(N)_{\mathbf{F}_p}$ is the Frobenius endomorphism, then as in the proof of Proposition 3.15, the action of Frobenius substitution φ_p on $V_\ell J_1(N)_{\mathbf{F}_p}$ is the same as the action of F on $V_\ell J_1(N)_{\mathbf{F}_p}$. Thus, it suffices to show

$$\det(1-Ft : V_\ell J_1(N)_{\mathbf{F}_p}) = 1 - T_p t + p\langle p\rangle t^2.$$

Let $V : J_1(N)_{\mathbf{F}_p} \to J_1(N)_{\mathbf{F}_p}$ be the dual of F. V is the pullback F^* by the morphism $F : X_1(N)_{\mathbf{F}_p} \to X_1(N)_{\mathbf{F}_p}$, and we have $FV = VF = p$.

LEMMA 9.18. *Let $N \geq 1$ be an integer, and let p be a prime number not dividing N.*

(1) *The following relation of endomorphisms of $J_1(N)_{\mathbf{F}_p}$ holds*

$$T_p = F + \langle p \rangle V. \tag{9.13}$$

(2) *Let ζ_N be an Nth root of unity, and let $w = w_N$ be the Atkin–Lehner involution defined by ζ_N. Then the following relation of endomorphisms of $J_1(N)_{\mathbf{F}_p(\zeta_N)}$ holds*

$$Vw = w\langle p \rangle V.$$

The relation (9.13) is called the *congruence relation.*

PROOF. (1) Since p is a prime, we have $I_1(N,p) = X_{1,0}(N,p)$. If $s, t : X_{1,0}(N,p) \to X_1(N)$ are natural morphisms, we have $T_p = t_* \circ s^* : J_1(N) \to J_{1,0}(N,p) \to J_1(N)$ by the definition of Hecke operators. By Theorem 8.76, $X_{1,0}(N,p)$ is semistable at p. Let $J_{1,0}(N,p)^{\mathfrak{a}}_{\mathbf{F}_p}$ be the abelian part of $J_{1,0}(N,p)^0_{\mathbf{F}_p}$. By Theorem A.49(1), $t_* : J_1(N,p) \to J_1(N)$ induces $J_1(N,p)^{\mathfrak{a}}_{\mathbf{F}_p} \to J_1(N)_{\mathbf{F}_p}$, and the Hecke operator $T_p : J_1(N)_{\mathbf{F}_p} \to J_1(N)_{\mathbf{F}_p}$ is the composition $J_1(N)_{\mathbf{F}_p} \to J_{1,0}(N,p)^{\mathfrak{a}}_{\mathbf{F}_p} \to J_1(N)_{\mathbf{F}_p}$.

By Theorem 8.76 and Corollary D.21, the morphism

$$(j_0^*, j_1^*) : J_1(N,p)^{\mathfrak{a}}_{\mathbf{F}_p} \longrightarrow J_1(N)_{\mathbf{F}_p} \times J_1(N)_{\mathbf{F}_p}$$

induced by $j_0, j_1 : X_1(N)_{\mathbf{F}_p} \to X_1(N,p)_{\mathbf{F}_p}$ is an isomorphism. Since the composition $t_* \circ (j_0^*, j_1^*) : J_1(N)_{\mathbf{F}_p} \times J_1(N)_{\mathbf{F}_p} \to J_1(N)_{\mathbf{F}_p}$ equals $(t_* \circ j_{0*}, t_* \circ j_{1*})$, $T_p = t_* \circ s^* : J_1(N)_{\mathbf{F}_p} \to J_1(N)_{\mathbf{F}_p}$ equals $(t \circ j_0)_* \circ (s \circ j_0)^* + (t \circ j_1)_* \circ (s \circ j_1)^*$. Hence, it suffices show

$$s \circ j_0 = \mathrm{id}, \qquad s \circ j_1 = F,$$
$$t \circ j_0 = F, \qquad t \circ j_1 = \langle p \rangle.$$

Since $j_0 : X_1(N)_{\mathbf{F}_p} \to X_1(N,p)_{\mathbf{F}_p}$ maps $[(E,P)]$ to $[(E,P,\operatorname{Ker} F)]$, we have $s \circ j_0 = \mathrm{id}$ and $t \circ j_0 = F$. Since $j_1 : X_1(N)_{\mathbf{F}_p} \to X_1(N,p)_{\mathbf{F}_p}$ maps $[(E,P)]$ to $[(E^{(p)}, P^{(p)}, \operatorname{Ker} V)]$, we have $s \circ j_1 = F$, and since $FV = p$, we have $t \circ j_1 = \langle p \rangle$.

(2) Each side is the pullback of an endomorphism of $X_1(N)_{\mathbf{F}_p}$, $w^{-1} \circ F$ and $F \circ \langle p \rangle^{-1} \circ w^{-1}$, respectively. Thus, it suffices to show $w \circ F = F \circ w \circ \langle p \rangle$. For an elliptic curve E over $\mathbf{F}_p(\zeta_N)$ and its section P of order N, let Q be a section of order N satisfying $(P,Q)_N = \zeta_N$. Then, we have $(P^{(p)}, Q^{(p)})_N = \zeta_N^p$. Hence, we have $w \circ F(E,P) = w(E^{(p)}, P^{(p)}) = (E^{(p)}/\langle P^{(p)} \rangle, p^{-1}Q^{(p)})$, and thus $w \circ F = \langle p \rangle^{-1} \circ F \circ w$.

On the other hand, since we have $F \circ w \circ \langle p \rangle = F \circ \langle p \rangle^{-1} \circ w = \langle p \rangle^{-1} \circ F \circ w$, we conclude that $w \circ F = F \circ w \circ \langle p \rangle$. ☐

We now come back to the proof of Theorem 9.16. Since $F \circ V = p$, we have

$$(1 - Ft)(1 - \langle p \rangle Vt) = 1 - T_p t + p\langle p \rangle t^2$$

by Lemma 9.18. Taking the determinant of each side, we obtain

$$\det(1 - Ft : V_\ell J_1(N)_{\mathbf{F}_p}) \det(1 - Vt : V_\ell J_1(N)_{\mathbf{F}_p}) = (1 - T_p t + p\langle p \rangle t^2)^2.$$

As in (9.9), the composition $V_\ell J_1(N)_{\mathbf{F}_p} \to \mathrm{Hom}(V_\ell J_1(N)_{\mathbf{F}_p}, \mathbf{Q}_\ell)$ of the limit of the isomorphism (D.15) and the transpose of the Atkin–Lehner involution w_N^* is an isomorphism of $T_1(N)_{\mathbf{Q}_\ell}$-modules. By Lemma 9.18(2), this isomorphism maps the action of F to the action of the transpose of $\langle p \rangle V$, we have $\det(1 - Ft : V_\ell J_1(N)_{\mathbf{F}_p}) = \det(1 - \langle p \rangle Vt : V_\ell J_1(N)_{\mathbf{F}_p})$. Thus, we have

$$\det(1 - Ft : V_\ell J_1(N)_{\mathbf{F}_p})^2 = (1 - T_p t + p\langle p \rangle t^2)^2.$$

If we regard $\det(1 - Ft), 1 - T_p t + p\langle p \rangle t^2 \in 1 + T_1(N)[[t]] \subset T_1(N)[[t]]^\times$, we obtain $\det(1 - Ft) = 1 - T_p t + p\langle p \rangle t^2$ by taking the square root of each side. ☐

COROLLARY 9.19. *Let ℓ be a prime number, and let K be a finite extension of $\mathbf{Q}_\ell$. For an ℓ-adic representation $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(K)$ and an integer $N \geq 1$, the following conditions* (1) *and* (2) *are equivalent.*

(1) *ρ is modular of level N.*
(2) *ρ is isomorphic to a subrepresentation of $V_\ell J_0(N) \otimes_{\mathbf{Q}_\ell} K$.*

PROOF. The reduced Hecke algebra $T_0'(N)_K$ is isomorphic to the product ring $\prod_{f \in \Phi(N)_K} K_f$. Thus, $V_\ell J_0(N) \otimes_{\mathbf{Q}_\ell} K$ is decomposed into the direct sum $\bigoplus_{f \in \Phi(N)_K} V_\ell J_0(N) \otimes_{T_0'(N)_{\mathbf{Q}_\ell}} K_f$. By Theorems 9.13 and 3.18(2), the semisimplification of $V_\ell J_0(N) \otimes_{T_0'(N)_{\mathbf{Q}_\ell}} K_f$ is the sum of ℓ-adic representations associated with f. The assertion follows from this immediately. ☐

As a matter of fact, we can prove that $V_\ell J_0(N) \otimes_{\mathbf{Q}_\ell} K$ is semisimple using Proposition 9.27 for example. However we do not prove it in this book.

If we let $p = \ell$ in Corollary 9.17, the following holds. If V is a good p-adic representation of $G_{\mathbf{Q}_p}$, a filtered $\mathbf{Q}_p[F, V]$-module $D(V)$ is defined as in §C.2. If A is an abelian variety over $\mathbf{Q}_p$ having good reduction at p and $V = V_p A$, then we have $D(V) = D(A_{\mathbf{F}_p})$.

COROLLARY 9.20. *Let p be a prime number, and let K be a finite extension of $\mathbf{Q}_p$. Let $N \geq 1$ be an integer relatively prime to p, $f \in S_1(N)_K$ a primary form of lever N, character ε, with K coefficients. Let V_f be the tensor product $V_pJ_1(N) \otimes_{T_1(N)_{\mathbf{Q}_p}} K$ with respect to the ring homomorphism $T_1(N)_{\mathbf{Q}_\ell} \to K$ defined by f.*

(1) *The restriction of V_f to $G_{\mathbf{Q}_p}$ is a good p-adic representation, and we have*

$$\det(1 - Ft : D(V_f)) = 1 - a_p(f)t + \varepsilon(p)pt^2.$$

The subspace $D(V_f)' \subset D(V_f)$ is one dimensional over K.

(2) *The restriction $V_f|_{G_{\mathbf{Q}_p}}$ of V_f to $G_{\mathbf{Q}_p}$ is ordinary if and only if $a_p(f)$ is a p-adic unit. Suppose $a_p(f)$ is a p-adic unit, and we write $1 - a_p(f)t + \varepsilon(p)pt^2 = (1 - \alpha t)(1 - p\beta t)$, where α and β are also p-adic units. We denote simply by α and β the unramified characters of $G_{\mathbf{Q}_p}$ whose value at φ_p are α and β, respectively. Let χ be the p-adic cyclotomic character. Then, $V_f|_{G_{\mathbf{Q}_p}}$ is an extension of α by $\beta \cdot \chi$.*

PROOF. By Theorem C.6(3), the submodule $D(V_pJ_1(N))'$ of the $T_1(N)_{\mathbf{Q}_p}$-module $D(V_pJ_1(N))$ equals $S_1(N)_{\mathbf{Q}_p}$ as a $T_1(N)_{\mathbf{Q}_p}$-module. Also by Theorem C.6(3), the quotient $D(V_pJ_1(N))/D(V_pJ_1(N))'$ is $\mathrm{Hom}(S_1(N)_{\mathbf{Q}_p}, \mathbf{Q}_p)$ as a $T_1(N)_{\mathbf{Q}_p}$-module. Thus, both $D(V_pJ_1(N))'$ and $D(V_pJ_1(N))/D(V_pJ_1(N))'$ are free $T_1(N)_{\mathbf{Q}_p}$-modules of rank 1. Hence, $D(V_pJ_1(N)) = D(J_1(N))$ is a free $T_1(N)_{\mathbf{Q}_p}$-module of rank 2. By Lemma 9.18(1), we have

$$\det\bigl(1 - Ft : D(V_pJ_1(N))\bigr)\det\bigl(1 - \langle p\rangle Vt : D(V_pJ_1(N))\bigr) = (1 - T_pt + p\langle p\rangle t^2)^2.$$

By Lemma 9.18(2), using Theorem C.2 for $k = \mathbf{F}_p(\zeta_N)$, we see

$$\det\bigl(1 - Ft : D(V_pJ_1(N))\bigr) = \det\bigl(1 - \langle p\rangle Vt : D(V_pJ_1(N))\bigr)$$

in the same way as the proof of Theorem 9.16. Hence, we have

$$\det(1 - Ft : D(V_pJ_1(N))) = 1 - T_pt + p\langle p\rangle t^2.$$

Since $D(V_f) = D(V_pJ_1(N)) \otimes_{T_1(N)_{\mathbf{Q}_p}} K$, this is a two-dimensional K-vector space, and $\det(1 - Ft : D(V_f)) = 1 - a_p(f)t + \varepsilon(p)pt^2$. $D(V_f)' = S_1(N)_{\mathbf{Q}_p} \otimes_{T_1(N)_{\mathbf{Q}_p}} K$ is one dimensional.

(2) Clear from (1) and Corollary C.8. □

THEOREM 9.21. *Let K be a field of characteristic 0, let $f \in S_1(N)_K$ be a primary form with K coefficients, let ε be the character of f, and let $p \nmid N$ be a prime number. If we write $1 - a_p(f)t + \varepsilon(p)pt^2 = (1-\alpha t)(1-\beta t)$, then both α and β are algebraic integers and the absolute value of any of their conjugates is $\sqrt{p}$.*

PROOF. Similarly to Corollary 9.3, $a_p(f)$ is an algebraic integer, and so are α and β. Replacing K by its subfield $K_f = \mathbf{Q}(a_n(f), n \geq 1)$, we may assume K is a number field. Take a prime number different from p. Replacing K by its completion at the place dividing ℓ, we may assume K is a finite extension of $\mathbf{Q}_\ell$.

By Theorem 9.16, α and β are the eigenvalues of the action of the Frobenius substitution φ_p on $V_\ell J_1(N)_{\mathbf{F}_p}$. The eigenvalues of the action of the Frobenius substitution φ_p on $V_\ell J_1(N)_{\mathbf{F}_p}$ are the eigenvalues of the action of the Frobenius morphism $F : X_1(N)_{\mathbf{F}_p} \to X_1(N)_{\mathbf{F}_p}$ on the étale cohomology group $H^1(X_1(N)_{\overline{\mathbf{F}}_p}, \mathbf{Q}_\ell)$. Thus, by the Weil conjecture, any of the complex conjugates of α and β has the absolute value $\sqrt{p}$. ☐

Theorem 2.47 follows immediately from Theorem 9.21.

9.3. Modular mod ℓ representations and non-Eisenstein ideals

In this section, we give relations between modular mod ℓ representations and maximal ideals of Hecke algebras with $\mathbf{Z}$ coefficients or the torsion points of the Jacobian of modular curves. We first give the correspondence between modular mod ℓ representations and maximal ideals of Hecke algebras with $\mathbf{Z}$ coefficients.

LEMMA 9.22. *Let ℓ be an odd prime number, and let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$. Let $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be an absolutely irreducible continuous representation, and let $N \geq 1$. Then, the following conditions* (i) *and* (ii) *are equivalent.*

(i) *$\bar{\rho}$ is modular of level N.*
(ii) *There exists a ring homomorphism $\bar{\varphi} : T_0(N)_{\mathbf{Z}} \to \mathbf{F}'$ to a finite extension $\mathbf{F}'$ of $\mathbf{F}$ such that*

$$\det(1 - \bar{\rho}(\varphi_p)t) = 1 - \bar{\varphi}(T_p)t + pt^2$$

for almost all prime numbers $p \nmid N$.

PROOF. Let K be a finite extension of $\mathbf{Q}_\ell$, let $f \in S_0(N)_K$ be a primary form, and let $\varphi_f : T_0(N)_{\mathbf{Q}} \to K$ be the ring homomorphism defined by f. If $\mathbf{F}_K$ is the residue field of K, $\varphi_f : T_0(N)_{\mathbf{Z}} \to K$ induces a homomorphism $\bar{\varphi}_f : T_0(N)_{\mathbf{Q}} \to \mathbf{F}_K$ and $\bar{\varphi}_f(T_p) \equiv a_p(f)$ for all prime numbers p.

Conversely, let $\mathbf{F}'$ be a finite extension of $\mathbf{F}$, and let $\bar{\varphi} : T_0(N)_{\mathbf{Z}} \to \mathbf{F}'$ be a ring homomorphism. Let $\mathfrak{m}$ be the maximal ideal $\operatorname{Ker}\bar{\varphi}$ of $T_0(N)_{\mathbf{Z}}$. Take a maximal ideal $\mathfrak{m}'$ of the integral closure A of $T_0(N)_{\mathbf{Z}}$ lying above $\mathfrak{m}$. Let $\mathcal{O}$ be the completion of A at $\mathfrak{m}'$, and let K be its field of fractions. K is a finite extension of $\mathbf{Q}_\ell$, and $\mathcal{O}$ is its ring of integers. Let f be a primary form corresponding to the ring homomorphism $T_0(N)_{\mathbf{Z}} \to K$, and replace $\mathbf{F}'$ by the compositum with the residue field $\mathbf{F}_K$ of K. We have $\bar{\varphi}_f(T_p) \equiv a_p(f)$ for all prime numbers p. The assertion now follows immediately from this. □

COROLLARY 9.23. *Let ℓ be an odd prime number, let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$, and let $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be an absolutely irreducible continuous representation. Let $N \geq 1$ be an integer, and let $\bar{\varphi} : T_0(N)_{\mathbf{Z}} \to \mathbf{F}$ be a ring homomorphism such that $\bar{\rho}$ is unramified at almost all prime numbers $p \nmid N$ and satisfies $\det(1 - \bar{\rho}(\varphi_p)t) = 1 - \bar{\varphi}(T_p)t + pt^2$. Then, the following hold.*

(1) *For all prime numbers $p \nmid N\ell$, $\bar{\rho}$ is unramified at p, and we have*
$$\det(1 - \bar{\rho}(\varphi_p)t) = 1 - \bar{\varphi}(T_p)t + pt^2.$$

(2) *If $\ell \nmid N$, $\bar{\rho}$ is good at ℓ. If $D(\rho)$ is the F-module obtained by applying Theorem C.6 to the restriction of $\bar{\rho}$ to $G_{\mathbf{Q}_\ell}$, we have*
$$\det(1 - Ft : D(\bar{\rho})) = 1 - \bar{\varphi}(T_\ell)t + \ell t^2.$$
Moreover, if $\bar{\rho}$ is good and ordinary at ℓ, then $\mathrm{Tr}(F : D(\bar{\rho})) = \bar{\varphi}(T_\ell)$ equals the value $\bar{\rho}_{I_\ell}(\varphi_\ell) \in \mathbf{F}^\times$ at the Frobenius substitution φ_ℓ of the unramified character $\bar{\rho}_{I_\ell}$ defined by the coinvariant quotient of ρ by the inertia group I_ℓ.

PROOF. (1) Clear from the proofs of Lemmas 9.22 and 3.26.
(2) Clear from Corollary 9.20 and the proof of (1). □

DEFINITION 9.24. Let $N \geq 1$ be an integer, and let $\mathfrak{m}$ be a maximal ideal of the Hecke algebra $T_0(N)_{\mathbf{Z}}$. Let $\mathbf{F}_{\mathfrak{m}} = T_0(N)_{\mathbf{Z}}/\mathfrak{m}$. We say that $\mathfrak{m}$ is an *Eisenstein ideal* if there exists an integer $M \geq 1$ and characters $\alpha, \beta : (\mathbf{Z}/M\mathbf{Z})^\times \to \mathbf{F}_{\mathfrak{m}}^\times$ such that
$$T_p \equiv \alpha(p) + \beta(p) \bmod \mathfrak{m}$$
for almost all prime numbers $p \nmid NM$.

If $\mathfrak{m}$ is not an Eisenstein ideal, we say that $\mathfrak{m}$ is a *non-Eisenstein ideal*.

EXAMPLE 9.25. The maximal ideal (5) of $T_0(11)_{\mathbf{Z}} = \mathbf{Z}$ is an Eisenstein ideal by Example 9.15. If $\ell \geq 3$ and $\ell \neq 5$, then by Proposition 4.3, the mod ℓ representation defined by the ℓ-torsion points of $E = X_0(11)$ is irreducible. Thus, by Proposition 9.26 below, the maximal ideal (ℓ) of $T_0(11)_{\mathbf{Z}}$ is non-Eisenstein.

A maximal ideal of a Hecke algebra with $\mathbf{Z}$ coefficients corresponds to a modular irreducible mod ℓ representation if and only if it is a non-Eisenstein ideal.

PROPOSITION 9.26. *Let $N \geq 1$ be an integer, and let ℓ be an odd prime number. Let $\mathfrak{m}$ be a maximal ideal of the Hecke algebra $T_0(N)_{\mathbf{Z}}$ containing ℓ, and let $\mathbf{F}_{\mathfrak{m}} = T_0(N)_{\mathbf{Z}}/\mathfrak{m}$ be the residue field. Then, the following conditions* (i) *and* (ii) *are equivalent.*

(i) *There exist a finite extension $\mathbf{F}$ of the residue field $\mathbf{F}_{\mathfrak{m}}$ and a modular irreducible representation $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ of level N satisfying*

$$\det(1 - \bar{\rho}(\varphi_p)t) \equiv 1 - T_p t + p t^2 \bmod \mathfrak{m} \tag{9.14}$$

for almost all prime numbers $p \nmid N$.

(ii) *$\mathfrak{m}$ is a non-Eisenstein ideal.*

PROOF. (i) $\Rightarrow$ (ii). Let $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be a modular irreducible representation satisfying condition (i). Suppose $\mathfrak{m}$ is an Eisenstein ideal and we derive a contradiction. If $\mathfrak{m}$ is an Eisenstein ideal and the characters $\alpha, \beta : (\mathbf{Z}/M\mathbf{Z})^\times \to \mathbf{F}_{\mathfrak{m}}^\times$ satisfy

$$T_p \equiv \alpha(p) + \beta(p) \bmod \mathfrak{m}$$

for almost all prime ideals $p \nmid NM$, then, by Proposition 3.4(3), $\bar{\rho}$ is isomorphic to the direct sum of the characters $\alpha \oplus \beta$, which is a contradiction.

(ii) $\Rightarrow$ (i). As in the proof of Lemma 9.22, take a homomorphism $T_0(N)_{\mathbf{Z}} \to \mathcal{O}$ to the ring of integers of a finite extension K of $\mathbf{Q}_\ell$ such that $\mathfrak{m}$ is the inverse image of a maximal ideal of $\mathcal{O}$. Let $f \in S_0(N)_K$ be a primary form corresponding to $T_0(N)_{\mathbf{Z}} \to \mathcal{O} \subset K$, and let V be the ℓ-adic representation of $G_{\mathbf{Q}}$ associated with f. Take an $\mathcal{O}$-lattice L of V stable under the action of $G_{\mathbf{Q}}$, and let $\mathbf{F}$ be the residue field of $\mathcal{O}$. $\bar{V} = L \otimes_{\mathcal{O}} \mathbf{F}$ defines a mod ℓ representation $\bar{\rho}$. $\bar{\rho}$ satisfies (9.14) for almost all prime numbers $p \nmid N$. It suffices to show that if $\mathfrak{m}$ is a non-Eisenstein ideal, $\bar{\rho}$ is reducible.

Taking the contrapositive, we assume $\bar{\rho}$ is reducible and show $\mathfrak{m}$ is an Eisenstein ideal. If $\bar{\rho}$ is reducible, the semisimplification of $\bar{\rho}$ is the direct sum of characters $\alpha, \beta : G_{\mathbf{Q}} \to \mathbf{F}^{\times}$. It suffices to show the image of α and β are in $\mathbf{F}_{\mathfrak{m}}^{\times}$. If σ_{∞} is the complex conjugate, we have $\alpha\beta(\sigma_{\infty}) = -1, \alpha(\sigma_{\infty}) = \pm 1, \beta(\sigma_{\infty}) = \pm 1$, and thus we may assume $\alpha(\sigma_{\infty}) = 1, \beta(\sigma_{\infty}) = -1$. By (9.14) and Theorem 3.1, we have $\det(1 - \bar{\rho}(\sigma)t) \in \mathbf{F}_{\mathfrak{m}}[t]$ for any σ_{∞}. Thus, for any $\tau \in \mathrm{Gal}(\mathbf{F}/\mathbf{F}_{\mathfrak{m}})$, we have $\{\tau \circ \alpha, \tau \circ \beta\} = \{\alpha, \beta\}$. Since $\tau \circ \alpha(\sigma_{\infty}) = 1$, we have $\tau \circ \alpha = \alpha$, and $\tau \circ \beta = \beta$. Thus, the image of α and β are in $\mathbf{F}_{\mathfrak{m}}^{\times}$, and $\mathfrak{m}$ is an Eisenstein ideal. ☐

In general, for a two-dimensional irreducible representation, we have the following.

PROPOSITION 9.27. *Let F be a field, let G be a group, and let $\rho : G \to \mathrm{GL}_2(F)$ be an absolutely irreducible representation. Let $V = F^2$ be the representation space of ρ. Let W be a finite-dimensional representation of G over F, and suppose the action of each $g \in G$ on W satisfies $g^2 - \mathrm{Tr}(\rho(g)) \cdot g + \det \rho(g) = 0$. Then, W is isomorphic to the product of copies of V as a representation of G.*

PROOF. The ring homomorphism from the group algebra $\rho : F[G] \to M_2[F]$ induced by $\rho : G \to \mathrm{GL}_2(F)$ is denoted also by ρ. Since $\rho : G \to \mathrm{GL}_2(F)$ is absolutely irreducible, $\rho : F[G] \to M_2(F)$ is surjective. Let J be the two-sided ideal $(g^2 - \mathrm{Tr}\,\rho(g) \cdot g + \det \rho(g); g \in G)$. The surjective homomorphism $F[G]/J \to M_2(F)$ induced by $\rho : F[G] \to M_2(F)$ is also denoted by ρ. Since the ring $M_2(F)$ is semisimple, and a simple $M_2(F)$-module is isomorphic to F^2, it suffices to show that the surjective homomorphism $\rho : F[G]/J \to M_2(F)$ is an isomorphism.

Define an anti-involution $*$ of $F[G]$ by $g^* = \det \rho(g) \cdot g^{-1}$. We have $*^2 = 1$. Since we have

$$\begin{aligned}&(g^2 - \mathrm{Tr}\,\rho(g) \cdot g + \det \rho(g))^* \\ &\qquad = \det \rho(g)^2 \cdot g^{-2} - \mathrm{Tr}\,\rho(g) \cdot \det \rho(g) \cdot g^{-1} + \det \rho(g) \\ &\qquad = \det \rho(g)(g^2 - \mathrm{Tr}\,\rho(g) \cdot g + \det \rho(g))g^{-2},\end{aligned}$$

the anti-involution $*$ preserves the ideal J. The anti-involution of $F[G]/J$ induced by $*$ is also denoted by $*$. Define an anti-involution $*$ of $M_2(F)$ by $A^* = \mathrm{Tr}(A) - A$. Since we have

$$g^* - (\mathrm{Tr}\,\rho(g) - g) = (g^2 - \mathrm{Tr}\,\rho(g) \cdot g + \det \rho(g))g^{-1} \in J,$$

the ring homomorphism $\rho : F[G]/J \to M_2(F)$ is compatible with the anti-involution $*$.

For any $x \in F[G]/J$, we have $x + x^* = \operatorname{Tr}\rho(x)$. We show $xx^* = \det\rho(x)$ for $x \in F[G]/J$. Since $\rho(xx^*) = \rho(x)\rho(x)^* = \det\rho(x)$, $xx^* = \det\rho(x)$ and $xx^* \in F$ are equivalent. Since

$$(x+y)(x+y)^* = xx^* + yy^* + xy^* + (xy^*)^* = xx^* + yy^* + \operatorname{Tr}\rho(xy^*),$$

$\{x \in F[G]/J | xx^* \in F\}$ is a linear subspace of $F[G]/J$. This subspace contains the image of G, which implies that it is the entire space. It follows immediately from this that the multiplicative group $(F[G]/J)^\times$ equals $\{x \in F[G]/J | \det\rho(x) \neq 0\}$.

We show $\rho : F[G]/J \to M_2(F)$ is injective. It suffices to show for $x \in \operatorname{Ker}\rho$, that the annihilator $\operatorname{Ann} x = \{y \in F[G]/J | yx = 0\}$ equals the entire $F[G]/J$. If $x \in \operatorname{Ker}\rho$, then $x^* = -x$. If $y \in F[G]/J$, we have $yx \in \operatorname{Ker}\rho$ and thus $yx = -(yx)^* = -x^*y^* = xy^*$. Hence for $y, z \in F[G]/J$, we have $yzx = x(yz)^* = xz^*y^* = zxy^* = zyx$. This implies $\operatorname{Ann} x \supset \{yz - zy \mid y, z \in F[G]/J\}$, and thus $\operatorname{Ann} x$ is a two-sided ideal of $F[G]/J$. Since $\rho(\operatorname{Ann} x)$ is a two-sided ideal of $M_2(F)$ containing $\{AB - BA | A, B \in M_2(F)\}$, it is the entire $M_2(F)$. Thus, $\operatorname{Ann} x$ contains an element y satisfying $\rho(y) = 1$. Since this y is an invertible element of $F[G]/J$, we have $\operatorname{Ann} x = F[G]/J$. This proves $x = 0$. ☐

We now give the relation between modular mod ℓ representations and the torsion points of the Jacobian of modular curves.

LEMMA 9.28. *Let $N \geq 1$ be an integer, let ℓ be an odd prime number, and let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of the Hecke algebra $T_0(N)_{\mathbf{Z}}$ containing ℓ. Let $\mathbf{F}$ be a finite extension of $\mathbf{F}_{\mathfrak{m}} = T_0(N)_{\mathbf{Z}}/\mathfrak{m}$, and let $\bar\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be a modular irreducible representation of level N satisfying*

$$\det(1 - \bar\rho(\varphi_p)t) \equiv 1 - T_p t + pt^2 \bmod \mathfrak{m}$$

for almost all prime numbers $p \nmid N$. Let $\overline{V} = \mathbf{F}^2$ be the representation space.

1. *$J_0(N)[\mathfrak{m}] = \{x \in J_0(N)(\overline{\mathbf{Q}}) \mid ax = 0$ for all $a \in \mathfrak{m}\}$ is not 0.*
2. *$J_0(N)[\mathfrak{m}] \otimes_{T_0(N)_{\mathbf{Z}}} \mathbf{F}$ is isomorphic to the direct sum of copies of $\overline{V}$ as a mod ℓ representation of $G_{\mathbf{Q}}$.*

PROOF. (1) We show $J_0(N)[\mathfrak{m}] \neq 0$. If we let $H_1(X_0(N)^{\mathrm{an}}, \mathbf{F}_\ell) = H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{F}_\ell$, then $J_0(N)[\mathfrak{m}]$ is isomorphic to

$$\begin{aligned} &H_1(X_0(N)^{\mathrm{an}}, \mathbf{F}_\ell)[\mathfrak{m}] \\ &\qquad = \{x \in H_1(X_0(N)^{\mathrm{an}}, \mathbf{F}_\ell) \mid ax = 0 \text{ for all } a \in \mathfrak{m}\} \end{aligned}$$

as $T_0(N)_{\mathbf{Z}}$-modules. Since $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ is a finitely generated $T_0(N)_{\mathbf{Z}}$-module and $T_0(N)_{\mathbf{Z}} \to \operatorname{End} H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ is injective, the localization $H_1(X_0(N)^{\mathrm{an}}, \mathbf{F}_\ell)_{\mathfrak{m}}$ is not 0. Since the localization $(T_0(N)_{\mathbf{Z}}/(\ell))_{\mathfrak{m}}$ is a finite local ring, we have $H_1(X_0(N)^{\mathrm{an}}, \mathbf{F}_\ell)[\mathfrak{m}] \neq 0$.

(2) Let $q \nmid N\ell$ be a prime number. By Lemma 9.18(1), we have the relation $T_q = F_q + V_q$ of the endomorphisms of $J_0(N)_{\mathbf{F}_q}$. Thus, as endomorphisms of $J_0(N)(\bar{\mathbf{F}}_q)$, we have $\varphi_q^2 - T_q\varphi_q + q = F_q^2 - T_qF_q + F_qV_q = 0$. Hence, for each prime number $q \nmid N\ell$, the action of the Frobenius substitution φ_q on $J_0(N)_{\mathbf{F}_q}[\mathfrak{m}]$ satisfies $\varphi_q^2 - T_q\varphi_q + q = 0$. If we let $W = J_0(N)[\mathfrak{m}] \otimes_{T_0(N)_{\mathbf{Z}}} \mathbf{F}$, then by Theorem 3.1, the assumption of Proposition 9.27 is satisfied. Thus, W is the direct sum of copies of $\overline{V}$. ☐

9.4. Level of modular forms and ramification of ℓ-adic representations

In §3 of Chapter 3, we state the following theorem on the level of modular forms and ramifications of ℓ-adic representations.

THEOREM 3.52. *Let $\mathcal{O}$ be the ring of integers of a finite extension K of $\mathbf{Q}_\ell$, and let f be a primitive form of level N with K coefficients. Let $\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O})$ be the ℓ-adic representation associated with f. For a prime number p, the following conditions* (i) *and* (ii) *in each of* (1) *and* (2) *are equivalent.*

(1) (i) $p \nmid N$.
  (ii) ρ_f *is good at* p.

(2) (i) $p^2 \nmid N$.
  (ii) ρ_f *is semistable at* p.

PROOF OF (i) $\Rightarrow$ (ii). By Theorem 8.63, $X_0(N)$ has good reduction at p if $p \nmid N$, has semistable reduction at p if $p^2 \nmid N$. Thus, the assertion follows from Corollary 9.17, Lemmas D.18, D.16, and Corollary D.22, and in the case $\ell = p$, together with the fact that $\det \rho_f$ is the ℓ-adic cyclotomic character. ☐

The rest of this section is devoted to the proof of (ii) $\Rightarrow$ (i). It uses the detailed structure of $X_{0,*}(N, r)$ studied in Proposition 8.57.

Let $N \geq 1$ be an integer, and let p be a prime number. Write $N = Mp^e$, where $M \geq 1$ is an integer relatively prime to p. If $e = 0$, we have nothing to prove. So, we assume $e \geq 1$. For an integer $0 \leq k \leq e$, the finite morphism of modular curves $s_{p^k} : X_0(Mp^e) \to X_0(M)$ (8.65) is denoted by $s_k : X_0(Mp^e) \to X_0(M)$ in this section. If $e = 1$, $s_0, s_1 : X_0(N) \to X_0(M)$ are the same as $s, t : I_0(M, p) \to X_0(M)$, which appeared in the definition of Hecke operators. Similarly, for an integer $0 \leq k < e$, the morphism $s_{p^k} : X_0(Mp^e) \to X_0(Mp)$ is denoted by $t_k : X_0(Mp^e) \to X_0(Mp)$.

Let $r \geq 3$ be an integer relatively prime to $N = Mp^e$. For an integer $k \in \mathbf{Z}$, let $\sigma^*_{p^k}$ be the automorphism of $\operatorname{Spec} \mathbf{Z}[\frac{1}{r}, \zeta_r]$ defined by $p^k \in (\mathbf{Z}/r\mathbf{Z})^\times = \operatorname{Gal}(\mathbf{Q}(\zeta_r)/\mathbf{Q})$. For a scheme X over $\mathbf{Z}[\frac{1}{r}, \zeta_r]$, the fibered product $X \times_{\operatorname{Spec} \mathbf{Z}[\frac{1}{r}, \zeta_r] \swarrow \sigma^*_{p^k}} \operatorname{Spec} \mathbf{Z}[\frac{1}{r}, \zeta_r]$ is denoted by $X^{(p^k)}$. If X is a scheme over $\mathbf{Z}[\frac{1}{r}, \zeta_r]/(p)$ and if $k \geq 0$, then this notation coincides with the one in §8.1.

Similarly to $s_k : X_0(Mp^e) \to X_0(M)$, we define

$$\begin{array}{rccc} s_k : & X_{0,*}(Mp^e, r)_{\mathbf{Z}[\frac{1}{r}]} & \longrightarrow & X_{0,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]} \\ & (E, (C, C_{p^e}), \alpha) & \longmapsto & (E/C_{p^k}, C, \alpha) \end{array}$$

for $0 \leq k \leq e$. Here, for a cyclic group C_{p^e} of order p^e, C_{p^k} is its unique cyclic subgroup of order p^k, and for a cyclic subgroup C of order M and a basis α of $E[r]$, their images in E/C_{p^k} are also denoted by C and α. For $P, Q \in E[r]$, the Weil pairing satisfies (image of P, image of $Q)_{(E/C_{p^k})[r]} = (P, Q)^{p^k}_{E[r]}$. Thus, the diagram

$$\begin{tikzcd} X_{0,*}(Mp^e, r)_{\mathbf{Z}[\frac{1}{r}]} \arrow[r, "s_k"] \arrow[d] & X_{0,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]} \arrow[d] \\ \operatorname{Spec} \mathbf{Z}[\frac{1}{r}, \zeta_r] \arrow[r, "\sigma^*_{p^k}"] & \operatorname{Spec} \mathbf{Z}[\frac{1}{r}, \zeta_r] \end{tikzcd} \tag{9.15}$$

is commutative. By the commutative diagram (9.15), the horizontal arrow s_k defines a morphism $X_{0,*}(Mp^e, r)_{\mathbf{Z}[\frac{1}{r}]} \to X_{0,*}(M, r)^{(p^k)}_{\mathbf{Z}[\frac{1}{r}]}$ of schemes over $\operatorname{Spec} \mathbf{Z}[\frac{1}{r}, \zeta_r]$.

Similarly, for $0 \leq k < e$, define

$$\begin{array}{rccc} t_k : & X_{0,*}(Mp^e, r)_{\mathbf{Z}[\frac{1}{r}]} & \longrightarrow & X_{0,*}(Mp, r)_{\mathbf{Z}[\frac{1}{r}]} \\ & (E, (C, C_{p^e}), \alpha) & \longmapsto & (E/C_{p^k}, (C, C_{p^{k+1}}/C_{p^k}), \alpha). \end{array}$$

t_k defines a morphism $X_{0,*}(Mp^e,r)_{\mathbf{Z}[\frac{1}{r}]} \to X_{0,*}(Mp,r)^{(p^k)}_{\mathbf{Z}[\frac{1}{r}]}$ of schemes over $\operatorname{Spec}\mathbf{Z}[\frac{1}{r},\zeta_r]$. Define a morphism $\langle p\rangle : X_{0,*}(Mp^e,r)_{\mathbf{Z}[\frac{1}{r}]} \to X_{0,*}(Mp^e,r)_{\mathbf{Z}[\frac{1}{r}]}$ by sending a triple (E,C,α) to the triple $(E,C,\alpha\circ p)$. $\langle p\rangle$ defines a morphism $\langle p\rangle : X_{0,*}(Mp^e,r)_{\mathbf{Z}[\frac{1}{r}]} \to X_{0,*}(Mp^e,r)^{(p^2)}_{\mathbf{Z}[\frac{1}{r}]}$ of schemes over $\operatorname{Spec}\mathbf{Z}[\frac{1}{r},\zeta_r]$.

In what follows, we choose a maximal ideal $\mathfrak{p}$ of $\mathbf{Z}[\zeta_r]$ lying above (p), and we denote by $\mathbf{F}_p(\zeta_r)$ its residue field $\mathbf{Z}[\zeta_r]/\mathfrak{p}$.

PROPOSITION 9.29. *Let p be a prime number, let $M\geq 1$ be an integer relatively prime to p, and let $r\geq 3$ be an integer relatively prime to $N=Mp^e$.*

(1) *To the abelian part $J_{0,*}(Mp^e,r)^{\mathrm{a}}_{\mathbf{F}_p(\zeta_r)}$, the morphism of abelian varieties $s_k^* : J_{0,*}(M,r)^{(p^k)} \to J_{0,*}(Mp^e,r)$ over $\mathbf{Q}(\zeta_r)$ induces an isogeny*

$$\bigoplus_{k=0}^{e} s_k^* : \prod_{k=0}^{e} J_{0,*}(M,r)^{(p^k)}_{\mathbf{F}_p(\zeta_r)} \longrightarrow J_{0,*}(Mp^e,r)^{\mathrm{a}}_{\mathbf{F}_p(\zeta_r)}. \tag{9.16}$$

(2) *To the torus part $J_{0,*}(Mp^e,r)^{\mathrm{t}}_{\mathbf{F}_p(\zeta_r)}$, the morphism of abelian varieties $s_k^* : J_{0,*}(M,r)^{(p^k)} \to J_{0,*}(Mp^e,r)$ over $\mathbf{Q}(\zeta_r)$ induces an isogeny*

$$\bigoplus_{k=0}^{e-1} t_k^* : \prod_{k=0}^{e-1} J_{0,*}(Mp,r)^{(p^k)\,\mathrm{t}}_{\mathbf{F}_p(\zeta_r)} \longrightarrow J_{0,*}(Mp^e,r)^{\mathrm{t}}_{\mathbf{F}_p(\zeta_r)}. \tag{9.17}$$

PROOF. (1) Suppose $a\leq e=a+b$. The morphism $j_a : X_{0,*}(M,r)_{\mathbf{F}_p} \to X_{0,*}(N,r)_{\mathbf{F}_p}$ is defined by

$$(E,C,\alpha)\longmapsto\begin{cases}(E,(C,\operatorname{Ker}V^aF^b),\alpha) & a\leq b,\\ (E^{(p^{a-b})},(C^{(p^{a-b})},\operatorname{Ker}V^aF^b),\alpha^{(p^{a-b})}) & b\leq a.\end{cases}$$

Thus, if $a\leq b$, then j_a is a morphism over $\mathbf{F}_p(\zeta_r)$. If $b\leq a$, the diagram

$$\begin{tikzcd} X_{0,*}(M,r)_{\mathbf{F}_p} \arrow[r, "j_a"] \arrow[d] & X_{0,*}(Mp^e,r)_{\mathbf{F}_p} \arrow[d] \\ \operatorname{Spec}\mathbf{F}_p(\zeta_r) \arrow[r, "\varphi_p^{a-b}"] & \operatorname{Spec}\mathbf{F}_p(\zeta_r) \end{tikzcd}$$

is commutative, and the closed immersion j_a defines a morphism $X_{0,*}(M,r)^{(p^{e-2a})}_{\mathbf{F}_p} \to X_{0,*}(N,r)_{\mathbf{F}_p}$ over $\mathbf{F}_p(\zeta_r)$.

By Proposition 8.73 and Corollary D.20, we obtain an isomorphism from the abelian part

$$\bigoplus_a j_a^* : J_{0,*}(Mp^e, r)^{\mathrm{a}}_{\mathbf{F}_p(\zeta_r)} \longrightarrow \prod_{a=0}^{e} J_{0,*}(M, r)^{(p^{\min(0,e-2a)})}_{\mathbf{F}_p(\zeta_r)}.$$

Thus, it suffices to show the morphism of abelian varieties

$$\bigoplus_{a,e} (s_k \circ j_a)^* : \prod_{k=0}^{e} J_{0,*}(M, r)^{(p^k)}_{\mathbf{F}_p(\zeta_r)} \to \prod_{a=0}^{e} J_{0,*}(M, r)^{(p^{\min(0,e-2a)})}_{\mathbf{F}_p(\zeta_r)}$$

is an isogeny. As in the proof of Lemma 9.18(1), $s_k \circ j_a$ is

$$\begin{cases} F^k & \text{if } a \le b, k \le b, \text{ i.e., } 2a \le e, a+k \le e, \\ \langle p \rangle^{k-b} F^{b-(k-b)} & \\ \quad = \langle p \rangle^{a+k-e} F^{2e-2a-k} & \text{if } a \le b \le k, \text{ i.e., } 2a \le e, a+k \ge e, \\ F^{a-b+k} = F^{2a+k-e} & \text{if } k \le b \le a, \text{ i.e., } 2a \ge e, a+k \le e, \\ \langle p \rangle^{k-b} F^{a-b+b-(k-b)} & \\ \quad = \langle p \rangle^{a+k-e} F^{e-k} & \text{if } b \le a, b \le k, \text{ i.e., } 2a \ge e, a+k \ge e. \end{cases}$$

As consequence, the determinant $\det(s_k \circ j_a)$ of the matrix $(s_k \circ j_a) \in M_{e+1}(\mathbf{Z}[F, \langle p \rangle])$ equals

$$(-1)^{\frac{e(e-1)}{2}} \prod_{1 \le a \le e/2} (\langle p \rangle - F^2) F^{e-a-1} \times \prod_{e/2 < a \le e} (\langle p \rangle - F^2) F^{a-1}.$$

Since $\langle p \rangle - F^2 : J_{0,*}(M, r)_{\mathbf{F}_p(\zeta_r)} \to J_{0,*}(M, r)^{(p^2)}_{\mathbf{F}_p(\zeta_r)}$ is étale, the determinant $\det(s_k \circ j_a)$ is an isogeny. Thus, $\bigoplus_{a,e}(s_k \circ j_a)^*$ is also an isogeny.

(2) Let X_e be the character group of the torus $J_{0,*}(Mp^e, r)^{\mathrm{t}}_{\mathbf{F}_p(\zeta_r)}$. Similarly, define X_1 for $J_{0,*}(Mp, r)^{\mathrm{t}}_{\mathbf{F}_p(\zeta_r)}$. It suffices to show that the homomorphism of $\mathbf{Z}$-modules $\bigoplus_k t_{k*} : X_e \to X_1^{\oplus e}$ induced by $\bigoplus_k t_k^* : \prod_{k=0}^{e-1} J_{0,*}(Mp, r)^{(p^k)} \to J_{0,*}(Mp^e, r)$ becomes an isomorphism after tensoring $\otimes \mathbf{Q}$.

We describe X_e and X_1 in terms of dual chain complexes. By Corollary 8.43, the field of constants of $X_{0,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]} \otimes_{\mathbf{Z}[\frac{1}{r}]} \mathbf{Q}$ is $\mathbf{Q}(\zeta_r)$. Thus, the proper smooth curve $X_{0,*}(M, r)_{\mathbf{Z}[\frac{1}{r}]}$ has a geometrically connected fiber $X_{0,*}(M, r)_{\overline{\mathbf{F}_p(\zeta_r)}}$ by Theorem A.16. Let $\Sigma = Y_{0,*}(M, r)^{\mathrm{ss}}_{\mathbf{F}_p(\zeta_r)}$ be the reduced closed subgroup scheme consisting of supersingular points, and let $\overline{\Sigma} = \Sigma(\overline{\mathbf{F}_p(\zeta_r)})$. By Proposition 8.73, the set of irreducible components of $X_{0,*}(Mp^e, r)_{\overline{\mathbf{F}_p(\zeta_r)}}$

is identified with $[0, e] = \{a \in \mathbf{N} \mid 0 \leq a \leq e\}$, and the set of the singular points of the reduced part $X_{0,*}(Mp^e, r)_{\mathbf{F}_p(\zeta_r),\mathrm{red}}$ is identified with Σ. Furthermore, the inverse image of Σ in the normalization of $X_{0,*}(Mp^e, r)_{\mathbf{F}_p(\zeta_r),\mathrm{red}}$ is identified with $\Sigma \times [0, e]$. Thus, if we let

$$\mathbf{Z}_0^{n+1} = \mathrm{Ker}(\mathbf{Z}^{n+1} \overset{\mathrm{sum}}{\to} \mathbf{Z}),$$

the dual chain complex of $X_{0,*}(Mp^e, r)_{\overline{\mathbf{F}_p(\zeta_r)}}$ is identified with $[(\mathbf{Z}_0^{e+1})^{\bar{\Sigma}} \to \mathbf{Z}^{e+1}]$. Thus, by Corollary D.20, the character group X_e is identified with $\mathrm{Ker}((\mathbf{Z}_0^{e+1})^{\bar{\Sigma}} \to \mathbf{Z}^{e+1})$. Similarly, the character group X_1 can be identified with $\mathrm{Ker}((\mathbf{Z}_0^{2})^{\bar{\Sigma}} \to \mathbf{Z}^{2})$. Since the rank of X_e and the rank of X_1^e are equal, it now suffices to show that $\bigoplus_k t_{k*} : X_e \to X_1^{\oplus e}$ is injective.

Similarly to $s_k \circ j_a$, $t_k \circ j_a$ is calculated as follows:

$$\begin{cases} j_0 \circ F^k & \text{if } a \leq b, k < b, \text{ i.e., } 2a \leq e, a + k < e, \\ j_1 \circ \langle p \rangle^{k-b} F^{b-(k-b)-1} & \text{if } a \leq b \leq k, \text{ i.e., } 2a \leq e, a + k \geq e, \\ \quad = j_1 \circ \langle p \rangle^{a+k-e} F^{2e-2a-k-1} & \\ j_0 \circ F^{a-b+k} = j_0 \circ F^{2a+k-e} & \text{if } k < b \leq a, \text{ i.e., } 2a \geq e, a + k < e, \\ j_1 \circ \langle p \rangle^{k-b} F^{a-b+b-(k-b)-1} & \text{if } b \leq a, k, \text{ i.e., } 2a \geq e, a + k \geq e. \\ \quad = j_1 \circ \langle p \rangle^{a+k-e} F^{e-k-1} & \end{cases}$$

For a supersingular elliptic curve, we have $[p] = F^2$. Thus, $\langle p \rangle : \Sigma \to \Sigma^{(p^2)}$ equals F^2. Hence, the mapping $t_{k*} : \Sigma \times [0, e] \to \Sigma \times [0, 1]$ induced by t_k is given by

$$t_k(x, a) = \begin{cases} (F^k(x), 0) & \text{if } 2a \leq e, a + k < e, \\ (F^{k-1}(x), 1) & \text{if } 2a \leq e, a + k \geq e, \\ (F^{2a+k-e}(x), 0) & \text{if } 2a \geq e, a + k < e, \\ (F^{2a+k-e-1}(x), 1) & \text{if } 2a \geq e, a + k \geq e. \end{cases}$$

Since the Frobenius morphism $F : \Sigma \to \Sigma^{(p)}$ is a bijection, the automorphism $\bigoplus_{2a \leq e} \mathrm{id} \oplus \bigoplus_{2a > e} F^{2a-e}$ of $\mathbf{Z}^{\bar{\Sigma} \times [0,e]}$ and the automorphism $\bigoplus_k F^k \oplus \bigoplus_k F^{k-1}$ of $\mathbf{Z}^{\bar{\Sigma} \times [0,e-1]} \oplus \mathbf{Z}^{\bar{\Sigma} \times [0,e-1]}$ are defined. The linear mapping $\mathbf{Z}^{[0,e]} \to \mathbf{Z}^{[0,1] \times [0,e-1]}$ that sends the standard basis $e_a \in \mathbf{Z}^{[0,e]}$ to $\sum_{a+k<e} e_{0,k} + \sum_{a+k \geq e} e_{1,k} \in \mathbf{Z}^{[0,1] \times [0,e-1]}$ is injective. The mapping $\bigoplus_k t_{k*} : \mathbf{Z}^{\bar{\Sigma} \times [0,e]} \to \bigoplus_{k=0}^{e-1} \mathbf{Z}^{\bar{\Sigma} \times [0,1]} = \mathbf{Z}^{\bar{\Sigma} \times [0,e-1]} \oplus \mathbf{Z}^{\bar{\Sigma} \times [0,e-1]}$ is obtained by composing the above automorphisms to the direct sum of injections. Thus, this is also injective. $\square$

COROLLARY 9.30. *Let p be a prime number, let $M \geq 1$ be an integer relatively prime to p, let $e \geq 0$ be an integer, and let $N = Mp^e$. Consider the morphisms of abelian varieties over $\mathbf{Q}$*

$$\bigoplus_k s_k^* : \bigoplus_{k=0}^{e} J_0(M) \longrightarrow J_0(Mp^e), \tag{9.18}$$

$$\bigoplus_k t_k^* : \bigoplus_{k=0}^{e-1} J_0(Mp) \longrightarrow J_0(Mp^e). \tag{9.19}$$

(1) *Let $\ell \neq p$ be a prime number. The linear mapping $\bigoplus_k s_k^* : V_\ell J_0(M)^{\oplus e+1} \to V_\ell J_0(N)$ is injective and induces an isomorphism*

$$V_\ell J_0(M)_{\mathbf{F}_p}^{\oplus e+1} \longrightarrow V_\ell J_0(N)_{\mathbf{F}_p}^{\mathrm{a}}. \tag{9.20}$$

The mapping of the torus parts defined by the morphism (9.19) *induces an isomorphism*

$$V_\ell J_0(Mp)_{\mathbf{F}_p}^{\mathrm{t}\oplus e} \longrightarrow V_\ell J_0(N)_{\mathbf{F}_p}^{\mathrm{t}}. \tag{9.21}$$

The invariant part $V_\ell J_0(N)^{I_p}$ by the inertia group is equal to the image of

$$(\bigoplus_k s_k^*, \bigoplus_k t_k^*) : V_\ell J_0(M)^{\oplus e+1} \oplus V_\ell J_0(Mp)^{I_p \ \oplus e} \longrightarrow V_\ell J_0(N), \tag{9.22}$$

and it is the direct sum of the abelian part $V_\ell J_0(N)^{\mathrm{a}}$ and the torus part $V_\ell J_0(N)^{\mathrm{t}}$.

(2) *The kernel of the morphism* (9.18) *is finite. The morphism* (9.18) *induces an isogeny $\bigoplus_k s_k^* : \bigoplus_{k=0}^{e} J_0(M)_{\mathbf{F}_p} \to J_0(Mp^e)_{\mathbf{F}_p}^{\mathrm{a}}$.*

(3) *The morphism* (9.19) *induces an isogeny of the torus parts $\bigoplus_k t_k^* : \bigoplus_{k=0}^{e-1} J_0(Mp)_{\mathbf{F}_p}^{\mathrm{t}} \to J_0(Mp^e)_{\mathbf{F}_p}^{\mathrm{t}}$.*

PROOF. (1) Let $r \geq 3$ be an integer relatively prime to $N = Mp^e$. Since $\mathbf{Q}(\zeta_r)$ is unramified at a prime ideal $\mathfrak{p}$ lying above p, it suffices to show the assertion after extending the base field to $\mathbf{Q}(\zeta_r)$. $X_0(Mp^e)_{\mathbf{Q}(\zeta_r)} = X_0(Mp^e)_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_r)$ is the quotient of $X_{0,*}(Mp^e, r)_{\mathbf{Q}}$ by $\mathrm{SL}_2(\mathbf{Z}/r\mathbf{Z})$. Thus, by Corollary D.14(2), the natural mappings

$$V_\ell J_0(Mp^e)_{\mathbf{F}_p(\zeta_r)}^{\mathrm{a}} \longrightarrow (V_\ell J_{0,*}(Mp^e, r)_{\mathbf{F}_p(\zeta_r)}^{\mathrm{a}})^{\mathrm{SL}_2(\mathbf{Z}/r\mathbf{Z})},$$
$$V_\ell J_0(Mp^e)_{\mathbf{F}_p(\zeta_r)}^{\mathrm{t}} \longrightarrow (V_\ell J_{0,*}(Mp^e, r)_{\mathbf{F}_p(\zeta_r)}^{\mathrm{t}})^{\mathrm{SL}_2(\mathbf{Z}/r\mathbf{Z})}$$

are isomorphisms. By the isogenies (9.16) and (9.17), we obtain the isomorphism (9.10) and (9.21) by taking the $\mathrm{SL}_2(\mathbf{Z}/r\mathbf{Z})$ invariant part. The remaining assertions follow immediately from the exact sequence (A.5)

$$0 \to V_\ell J_0(Mp^e)^{\mathrm{t}} \to V_\ell J_0(Mp^e)^{I_p} \to V_\ell J_0(Mp^e)^{\mathrm{a}} \to 0.$$

(2) By the isomorphism (9.20), $V_\ell J_0(M)^{\oplus e+1} \to V_\ell J_0(N)$ is injective, and the kernel of the morphism (9.18) is finite. By the isomorphism (9.20), $\bigoplus_k s_k^* : J_0(M)_{\mathbf{F}_p}^{e+1} \to J_0(Mp^e)_{\mathbf{F}_p}^{\mathrm{a}}$ is an isogeny.

(3) Clear from the isomorphism (9.21). $\square$

PROOF OF (ii) $\Rightarrow$ (i). We show the case $p \neq \ell$. The case $p = \ell$ is similar, and we omit the proof.

(1) Suppose a modular ℓ-adic representation V_f of level N is good at p, and we show V_f is modular of level M. By Corollary 9.19, we may assume V_f is a subrepresentation of $V_\ell J_0(N) \otimes K$. Let W be the image of $\bigoplus_k s_k^* : V_\ell J_0(M)^{\oplus e+1} \to V_\ell J_0(N)$. Then, we have $V_f^{I_p} = V_f$, and thus $V_f \subset V_\ell J_0(N)^{I_p} \otimes K$. We show $V_f \subset W \otimes K$. By Theorem 9.21, the eigenvalues of the action of φ_p on W are algebraic integers, and their complex absolute value equals $\sqrt{p}$. By Corollary 9.30(1), the eigenvalues of the action of φ_p on $V_\ell J_0(N)^{I_p}/W$ is p times a root of unity. On the other hand, we have $\det(\varphi_p : V_f) = p$. Thus, we have $V_f \subset W \otimes K$. Hence, by Theorem 3.18(2), V_f is isomorphic to an irreducible subrepresentation of $V_\ell J_0(M) \otimes K$. By Corollary 9.19, V_f is modular of level M.

(2) Suppose a modular ℓ-adic representation V_f of level N is semistable at p, and we show V_f is modular of level Mp. By Corollary 9.19, we may assume V_f is a subrepresentation of $V_\ell J_0(N) \otimes K$. Let W' be the image of $(\bigoplus_k s_k^*, \bigoplus_k t_k^*) : V_\ell J_0(M)^{\oplus e+1} \oplus V_\ell J_0(Mp)^{\oplus e} \to V_\ell J_0(N)$. Then, since $V_f^{I_p} \neq 0$, we have $V_f \cap (W' \otimes K) \neq 0$ by Corollary 9.30(1). Since V_f is irreducible, we have $V_f \subset W' \otimes K$. Thus, V_f is isomorphic to a subrepresentation of $V_\ell J_0(M) \otimes K$ or $V_\ell J_0(Mp) \otimes K$, and thus it is modular of level Mp. $\square$

Similarly to Theorem 3.52, we prove the following.

THEOREM 9.31. *Let p be a prime number N, let $M \geq 1$ be integers relatively prime to each other and not divisible by p. Let $e \geq 0$ be an integer. Let ℓ be a prime number, and let K be a finite extension of $\mathbf{Q}_\ell$. Let $f \in S_{1,0}(Mp^e, N)_K$ be a primary form with K coefficients, and let V_f be the ℓ-adic representation associated with f.*

(1) *The following conditions* (i) *and* (ii) *are equivalent.*
  (i) V_f *is good at* p.
  (ii) V_f *is modular of level* $\Gamma_{1,0}(M,N)$. *More precisely, there exists a primary form* $g \in S_{1,0}(M,N)_K$ *such that* V_f *is isomorphic to the* ℓ*-adic representation associated with* g.
(2) *The following conditions* (i) *and* (ii) *are equivalent.*
  (i) V_f *is semistable at* p.
  (ii) V_f *is modular of level* $\Gamma_{1,0}(M,Np)$. *More precisely, there exists a primary form* $g \in S_{1,0}(M,Np)_K$ *such that* V_f *is isomorphic to the* ℓ*-adic representation associated with* g.

PROOF. If $f \in S_{1,0}(M,Np^e)_K$, the proof is similar to that of Theorem 3.52, and we omit it here.

We reduce it to the case $f \in S_{1,0}(M,Np^e)_K$. It suffices to show $f \in S_{1,0}(M,Np^e)$ if V_f is semistable at p. We show in the case $\ell \neq p$. We omit the case $\ell = p$.

Suppose V_f is semistable at p. Then, $\deg \rho_f$ is unramified at p. On the other hand, by Theorem 9.16, $\det \rho_f$ is the product of the ℓ-adic cyclotomic character and the character of f, $\varepsilon_f : (\mathbf{Z}/Mp^e\mathbf{Z})^\times = \mathrm{Gal}(\mathbf{Q}(\zeta_{Mp^e})/\mathbf{Q}) \to K^\times$. Thus, the restriction of ε_f to $(\mathbf{Z}/p^e\mathbf{Z})^\times \subset (\mathbf{Z}/Mp^e\mathbf{Z})^\times$ is trivial. Hence, f is contained in the invariant part $S_{1,0}(Mp^e,N)^{(\mathbf{Z}/p^e\mathbf{Z})^\times}_K$. The invariant part $S_{1,0}(Mp^e,N)_K^{(\mathbf{Z}/p^e\mathbf{Z})^\times}$ is equal to $S_{1,0}(M,Np^e)_K$ since the quotient of $X_{1,0}(Mp^e,N)$ by the group $(\mathbf{Z}/p^e\mathbf{Z})^\times$ is $X_{1,0}(M,Np^e)$. This proves $f \in S_{1,0}(M,Np^e)_K$. □

As for the ramification at p of the Galois representation associated with a modular form of level $\Gamma_1(Mp)$, the following holds.

THEOREM 9.32. *Let* p *be a prime number, let* $M \geq 1$ *be an integer relatively prime to* p. *Let* $\ell \neq p$ *be a prime number, and let* K *be a finite extension of* $\mathbf{Q}_f$. *Let* $f \in S_1(Mp)_K$ *be a primary form with* K *coefficient, let* $\varepsilon : (\mathbf{Z}/Mp\mathbf{Z})^\times \to K^\times$ *be the character of* f, *and let* V_f *be the* ℓ*-adic representation associated with* f. *Assume the restriction* $\varepsilon|_{(\mathbf{Z}/p\mathbf{Z})^\times}$ *is nontrivial.*

Then, we have $a_p(f) \neq 0$. *Let* $\alpha : G_{\mathbf{Q}_p} \to K^\times$ *be the unramified character defined by* $\alpha(\varphi_p) = a_p(f)$, *and let* $\chi : G_{\mathbf{Q}} \to \mathbf{Q}_\ell^\times$ *be the* ℓ*-adic cyclotomic character. Then, the restriction of* V_f *to* $G_{\mathbf{Q}_p}$ *is the direct sum of the unramified character* α *and the ramified character* $(\chi \cdot \varepsilon)|_{G_{\mathbf{Q}_p}} \cdot \alpha^{-1}$.

We first show the consequence of Theorem 8.77

PROPOSITION 9.33. *Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p. Define an abelian variety J over $\mathbf{Q}$ to be the cokernel of the pullback $J = \mathrm{Coker}(J_{1,0}(M,p) \to J_1(Mp))$ of the natural map $X_1(Mp) \to X_{1,0}(M,p)$.*

(1) *The base change $J_{\mathbf{Q}(\zeta_p)} = J \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_p)$ has good reduction at the prime ideal $\mathfrak{p} = (\zeta_p - 1)$. If $J_\mathfrak{p}$ is the reduction* mod $\mathfrak{p}$ *of $J_{\mathbf{Q}(\zeta_p)}$, the closed immersions $j_0, j_1 : \overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p} \to X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\zeta_p]}$ (8.61) induce an isomorphism*

$$(j_0, j_1)^* : J_\mathfrak{p} \longrightarrow (\mathrm{Jac}\,\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p}/J_1(M)_{\mathbf{F}_p})^2. \tag{9.23}$$

(2) *Let ℓ be a prime number different from p, and let $V_\ell J_\mathfrak{p}^{I_p}$ be the invariant part by the action of the inertia group $I_p =$ $\mathrm{Gal}(\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p)$. Then, j_1^* induces an isomorphism*

$$j_1^* : V_\ell J_\mathfrak{p}^{I_p} \longrightarrow V_\ell\,\mathrm{Jac}\,\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p}/V_\ell J_1(M)_{\mathbf{F}_p}. \tag{9.24}$$

(3) *The isomorphism $(j_0, j_1)^*$ is compatible with the Hecke operators T_q $(q \neq p)$ and the diamond operators $\langle a \rangle$ $(a \in (\mathbf{Z}/M\mathbf{Z})^\times)$. The isomorphism j_1^* sends the action of the Hecke operator T_p to the action of the Frobenius homomorphism F.*

PROOF. (1) By Corollaries 8.78 and D.21, $J_1(Mp)_{\mathbf{Q}(\zeta_p)}$ has semistable reduction at $\mathfrak{p}$. Moreover, the character group of the torus part $J_1(Mp)^{\mathrm{t}}_{\mathbf{F}_\mathfrak{p}}$ of the mod $\mathfrak{p}$ reduction $J_1(Mp)_{\mathbf{F}_\mathfrak{p}}$ is naturally isomorphic to the character group of the torus part $J_{1,0}(M,p)^{\mathrm{t}}_{\mathbf{F}_p}$ of the mod $\mathfrak{p}$ reduction of $J_{1,0}(M,p)_{\mathbf{F}_p}$. Thus, the natural morphism $J_{1,0}(M,p)^{\mathrm{t}}_{\mathbf{F}_p} \to J_1(Mp)^{\mathrm{t}}_{\mathbf{F}_\mathfrak{p}}$ is an isomorphism, and $J_{\mathbf{Q}(\zeta_p)} =$ $\mathrm{Coker}(J_{1,0}(M,p)_{\mathbf{Q}(\zeta_p)} \to J_1(Mp)_{\mathbf{Q}(\zeta_p)})$ has good reduction at $\mathfrak{p}$. By the diagram (8.64), the isomorphisms from the abelian part $j_0^* \oplus j_1^*$: $J_1(Mp)^{\mathrm{a}}_{\mathbf{F}_\mathfrak{p}} \to \mathrm{Jac}\,\overline{\mathrm{Ig}}(Mp)^2_{\mathbf{F}_p}$ and $j_0^* \oplus j_1^* : J_{1,0}(M,p)^{\mathrm{a}}_{\mathbf{F}_p} \to J_1(M)^2_{\mathbf{F}_p}$ induce the isomorphism (9.23).

(2) By Theorem 8.77 and Corollary D.21, we obtain a commutative diagram

$$\begin{tikzcd}
J_{1,0,*}(M,p,r)^{\mathrm{a}}_{\mathbf{F}_p} \arrow[r] \arrow[d, "(j_0{,}j_1)^*"'] & J_{1,*}(Mp,r)^{\mathrm{a}}_{\mathbf{F}_p} \arrow[r] \arrow[d, "(j_0{,}j_1)^*"'] & J_{1,*}(Mp,r)^{\mathrm{a}}_{\mathbf{F}_\mathfrak{p}} \arrow[d, "(j_0{,}j_1)^*"] \\
J_{1,*}(M,r)^2_{\mathbf{F}_p} \arrow[r] & J_{1,*}(M,r)_{\mathbf{F}_p} \times \mathrm{Jac}\,\overline{\mathrm{Ig}}(Mp,r)_{\mathbf{F}_p} \arrow[r] & \mathrm{Jac}\,\overline{\mathrm{Ig}}(Mp,r)^2_{\mathbf{F}_p},
\end{tikzcd}$$

and the vertical arrows are isomorphisms. Taking the $\mathrm{SL}_2(\mathbf{Z}/r\mathbf{Z})$ invariant part of V_ℓ of these abelian varieties, we obtain the commutative diagram

$$\begin{tikzcd}
V_\ell J_{1,0}(M,p)^{\mathrm{a}}_{\mathbf{F}_p} \arrow[r] \arrow[d, "(j_0{,}j_1)^*"'] & V_\ell J_1(Mp)^{\mathrm{a}}_{\mathbf{F}_p} \arrow[r] \arrow[d, "(j_0{,}j_1)^*"'] & V_\ell J_1(Mp)^{\mathrm{a}}_{\mathbf{F}_p} \arrow[d, "(j_0{,}j_1)^*"] \\
V_\ell J_1(M)^2_{\mathbf{F}_p} \arrow[r] & V_\ell J_1(M)_{\mathbf{F}_p} \times V_\ell \operatorname{Jac}\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p} \arrow[r] & V_\ell \operatorname{Jac}\overline{\mathrm{Ig}}(Mp)^2_{\mathbf{F}_p},
\end{tikzcd}$$

and the vertical arrows are isomorphisms. By Corollary D.13(3), the natural morphism $V_\ell J_1(Mp)^{\mathrm{a}}_{\mathbf{F}_p} = (V_\ell J_1(Mp)^{\mathrm{a}}_{\mathbf{F}_p})^{I_p}$ is an isomorphism. Hence, we obtain the isomorphism

$$V_\ell J_{\mathrm{p}}^{I_p} \to V_\ell J_1(Mp)^{\mathrm{a}}_{\mathbf{F}_p}/V_\ell J_{1,0}(M,p)^{\mathrm{a}}_{\mathbf{F}_p} \xrightarrow{j_1^*} V_\ell \operatorname{Jac}\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p}/V_\ell J_1(M)_{\mathbf{F}_p}.$$

(3) We omit the proof. □

PROOF OF THEOREM 9.32. By Theorem 9.16, under the notation of Proposition 9.33, we may assume V_f is a subrepresentation of $V_\ell J \otimes_{\mathbf{Q}_\ell} K$. Thus, by Proposition 9.33(2), we have $V_f^{I_p} = V_f \cap (V_\ell(\operatorname{Jac}\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p}/J_1(M)_{\mathbf{F}_p}) \otimes_{\mathbf{Q}_\ell} K)$, and $V_f = V_f^{I_p} \oplus V_f/V_f^{I_p}$. If we write $T_1(Mp)_{\mathbf{Q}_p} = T_{1,0}(M,p)_{\mathbf{Q}_p} \times A$, then by Proposition 9.33 and Lemma 9.12(2), $V_\ell(\operatorname{Jac}\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p}/J_1(M)_{\mathbf{F}_p})$ is a free A-module of rank 1. Thus, both $V_f^{I_p}$ and $V_f/V_f^{I_p}$ are one dimensional. The action of the Frobenius substitution φ_p on $V_\ell \operatorname{Jac}\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p} \otimes_{\mathbf{Q}_\ell} K$ is the same as the action of the Frobenius homomorphism F, and in turn, the same as the action of the Hecke operator T_p by Proposition 9.33(3). Thus, the action of φ_p on the invariant part $V_f^{I_p} = V_f \cap (V_\ell(\operatorname{Jac}\overline{\mathrm{Ig}}(Mp)_{\mathbf{F}_p}/J_1(M)_{\mathbf{F}_p}) \otimes_{\mathbf{Q}_\ell} K)$ is the multiplication by $a_p(f)$. Hence, $a_p(f) \neq 0$. Since $\det \rho_f = \chi \cdot \varepsilon$, the representation $V_f|_{G_{\mathbf{Q}_p}}$ is the sum of the characters $\alpha : G_{\mathbf{Q}_p} \to K^\times$ and $(\chi \cdot \varepsilon)|_{G_{\mathbf{Q}_p}} \cdot \alpha^{-1}$. □

9.5. Old part

Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p. In the proof of Theorem 3.52, the natural morphisms

$$\begin{aligned}
&\oplus_k s_k^* : \bigoplus_{k=0}^{e} J_0(M) \longrightarrow J_0(Mp^e), \\
(9.25)\qquad & \\
&\oplus_k t_k^* : \bigoplus_{k=0}^{e-1} J_0(Mp) \longrightarrow J_0(Mp^e)
\end{aligned}$$

played an important role. In this section we study these morphisms in more detail. In general, if M is a proper factor of N, the image of the natural morphism $\bigoplus_d s_d^* : \bigoplus_{d|N/M} J_0(M) \to J_0(N)$ is called the *old part* of $J_0(N)$.

We first study the action of s_d^* on the q-expansion.

LEMMA 9.34. *Let $d, M, N \geq 1$ be integers, and suppose $dM \mid N$. The image of $f = \sum_{n=1}^{\infty} a_n q^n \in S_0(M)_{\mathbf{C}}$ by $s_d^* : S_0(M)_{\mathbf{C}} \to S_0(N)_{\mathbf{C}}$ is given by*

$$s_d^* f = \sum_{n=1}^{\infty} d a_n q^{dn}. \tag{9.26}$$

PROOF. Let $e : \Delta \to X_0(N)^{\mathrm{an}}$ be the morphism in Proposition 2.68(1). The morphism e is defined by the family of elliptic curves $E_q = \mathbf{C}^\times/q^{\mathbf{Z}}$ over $\Delta^* = \Delta - \{0\}$ and its cyclic subgroup μ_N. We denote the dth power mapping $\Delta \to \Delta$ also by s_d. By the dth power mapping $\mathbf{C}^\times/q^{\mathbf{Z}} \to \mathbf{C}^\times/q^{d\mathbf{Z}}$, the quotient E_q/μ_d is isomorphic to the pullback of E_q by $s_d : \Delta \to \Delta$, and μ_{Md}/μ_d is mapped to μ_M. Thus, the diagram

$$\begin{tikzcd}
\Delta \arrow[r, "e"] \arrow[d, "s_d"'] & X_0(N)^{\mathrm{an}} \arrow[d, "s_d"] \\
\Delta \arrow[r, "e"] & X_0(M)^{\mathrm{an}}
\end{tikzcd}$$

is commutative. Hence, we obtain $s_d^*(f\frac{dq}{q}) = \sum_{n=1}^{\infty} a_n q^{dn} \cdot \frac{dq^d}{q^d}$. □

From now on, as in the previous section, let p be a prime number, and for an integer $M \geq 1$, we denote simply by s_k the morphism of modular curves $s_{p^k} : X_0(Mp^k) \to X_0(M)$.

LEMMA 9.35. *Let p be a prime number, let $M \geq 1$ be an integer relatively prime to p, and let $e \geq 0$ be an integer. Let $N = Mp^e$.*

(1) *There is an isomorphism of curves $a : X_0(Mp^{e+1}) \to I_0(Mp^e, p)$ that makes the diagram*

$$\begin{tikzcd}
X_0(Mp^{e+1}) \arrow[r, "s_0"] \arrow[d, "s_1"'] \arrow[dr, "a"'] & X_0(Mp^e) \\
X_0(Mp^e) & I_0(Mp^e, p) \arrow[l, "s"'] \arrow[u, "t"']
\end{tikzcd} \tag{9.27}$$

commutative.

(2) *Suppose* $e \geq 2$. *Then, the diagram*

$$\begin{tikzcd} X_0(Mp^{e+1}) \arrow[r, "s_0"] \arrow[d, "s_1"'] & X_0(Mp^e) \arrow[d, "s_1"] \\ X_0(Mp^e) \arrow[r, "s_0"] & X_0(Mp^{e-1}) \end{tikzcd} \tag{9.28}$$

is commutative, and it induces an isomorphism $X_0(Mp^{e+1}) \to$ (*the normalization of* $X_0(Mp^e) \times_{X_0(Mp^{e-1})} X_0(Mp^e)$).

(3) *Suppose* $e \geq 1$, *and let* $w = w_p : X_0(Mp) \to X_0(Mp)$ *be the Atkin–Lehner involution. Then the diagram*

$$\begin{tikzcd} X_0(Mp^{e+1}) \amalg X_0(Mp^e) \arrow[r, "(s_0{,}\mathrm{id})"] \arrow[d, "(s_e{,}w\circ s_{e-1})"'] & X_0(Mp^e) \arrow[d, "s_e"] \\ X_0(Mp) \arrow[r, "s_0"] & X_0(M) \end{tikzcd} \tag{9.29}$$

is commutative, and it induces an isomorphism $X_0(Mp^{e+1}) \amalg X_0(Mp^e) \to$ (*the normalization of* $X_0(Mp^e) \times_{X_0(M)} X_0(Mp)$).

PROOF. (1) Define a morphism $a : X_0(Mp^{e+1}) \to I_0(Mp^e, p)$ by sending $(E, C_M, C_{p^{e+1}})$ to $(E/C_p, C_M, C_{p^{e+1}}/C_p, E[p]/C_p)$. The inverse morphism $I_0(Mp^e, p) \to X_0(Mp^{e+1})$ is obtained by sending (E, C_M, C_{p^e}, C) to $(E/C, C_M, [p]^{-1}C_{p^e}/C)$.

The lower left triangle of (9.27) is clearly commutative. Since the image of $C_{p^{e+1}}/C_p$ in $E = (E/C_p)/(E[p]/C_p)$ is C_{p^e}, the upper right triangle is also commutative.

(2) The commutativity is easy to prove. Since $X_0(Mp^{e+1}) \to$ (normalization of $X_0(Mp^e) \times_{X_0(Mp^{e-1})} X_0(Mp^e)$) is a morphism of coverings of degree p of $X_0(Mp^e)$, it is an isomorphism.

(3) Since $s_0 \circ w : X_0(Mp) \to X_0(M)$ equals s_q, the diagram (9.29) is commutative. The proof of the isomorphism is similar to (2). □

PROPOSITION 9.36. *Let p be a prime number, and let $M \geq 1$, $e \geq 1$ be integers. Let $N = Mp^e$. Define $U_p \in M_{e+1}(\mathrm{End}\, J_0(M))$ by*

$$U_p = \begin{pmatrix} 0 & 0 & & 0 & 0 \\ p & & & \vdots & \vdots \\ 0 & & & 0 & 0 \\ \vdots & & \ddots & 0 & -1 \\ 0 & & 0 & p & T_p \end{pmatrix} \tag{9.30}$$

if $p \nmid M$, *and*

$$(9.31) \qquad U_p = \begin{pmatrix} 0 & & 0 & 0 \\ p & & \vdots & \vdots \\ 0 & & \vdots & \vdots \\ \vdots & \ddots & 0 & 0 \\ 0 & 0 & p & T_p \end{pmatrix}$$

if $p \mid M$. *Then, the diagram*

$$(9.32) \qquad \begin{tikzcd} \bigoplus_{k=0}^{e} J_0(M) \arrow[r, "\oplus_k s_k^*"] \arrow[d, "U_p \times"'] & J_0(Mp^e) \arrow[d, "T_p"] \\ \bigoplus_{k=0}^{e} J_0(M) \arrow[r, "\oplus_k s_k^*"] & J_0(Mp^e) \end{tikzcd}$$

is commutative.

Proof. It suffices to show

$$(9.33) \qquad T_p \circ s_k^* = \begin{cases} p \cdot s_{k+1}^* & \text{if } 0 \leq k < e, \\ s_e^* \circ T_p - s_{e-1}^* & \text{if } k = e \text{ and } p \nmid M, \\ s_e^* \circ T_p & \text{if } k = e \text{ and } p|M. \end{cases}$$

By Lemma 9.35(1), we have $T_p = s_{0*} \circ s_1^*$ for $s_0, s_1 : X_0(Mp^{e+1}) \to X_0(Mp^e)$.

First, we show the case $k < e$. Since $s_k \circ s_1 : X_0(Mp^{e+1}) \to X_0(M)$ equals $s_{k+1} \circ s_0$, we have

$$T_p \circ s_k^* = s_{0*} \circ s_1^* \circ s_k^* = s_{0*} \circ s_0^* \circ s_{k+1}^* = p \cdot s_{k+1}^*.$$

Next, we show the case $k = e$. If $p \nmid M$, then by Lemma 9.35(3) and $s_0 = s_1 \circ w$, we have

$$\begin{aligned} s_e^* \circ T_p &= s_e^* \circ s_{0*} \circ s_1^* = (s_{0*} \circ s_e^* + s_{e-1}^* \circ w^*) \circ s_1^* \\ &= s_{0*} \circ s_{e+1}^* + s_{e-1}^* = T_p \circ s_e^* + s_{e-1}^*. \end{aligned}$$

If $p \mid M$, then by Lemma 9.35(2), we have

$$s_e^* \circ T_p = s_e^* \circ s_{0*} \circ s_1^* = s_{0*} \circ s_e^* \circ s_1^* = s_{0*} \circ s_1^* \circ s_e^* = T_p \circ s_e^*. \quad \square$$

Corollary 9.37. *Let p be a prime number, let $M \geq 1$ be an integer relatively prime to p, and let $e \geq 1$. Let $N = Mp^e$. Let*

$P_p(U) \in \mathcal{T}_0(M)_{\mathbf{Z}}[U]$ be the characteristic polynomial of the matrix U_p

$$P_p(U) = \det(U - U_p) = U^{e-1}(U^2 - T_pU + p). \tag{9.34}$$

1. *Sending $T_q \in \mathcal{T}_0(N)_{\mathbf{Z}}$ to T_q if $q \neq p$, and to U if $q = p$, we obtain a ring homomorphism*

$$\mathcal{T}_0(N)_{\mathbf{Z}} \longrightarrow \mathcal{T}_0(M)_{\mathbf{Z}}[U]/(P_p(U)). \tag{9.35}$$

2. *Regard $\bigoplus_{k=0}^{e} J_0(M)$ as a $\mathcal{T}_0(M)_{\mathbf{Z}}[U]/(P_p(U))$-module by defining the action of U as the multiplication of the matrix U_p in (9.30). Then, $\bigoplus_k s_k^* : \bigoplus_{k=0}^{e} J_0(M) \to J_0(Mp^e)$ is compatible with the ring homomorphism $\mathcal{T}_0(N)_{\mathbf{Z}} \to \mathcal{T}_0(M)_{\mathbf{Z}}[U]/(P_p(U))$ (9.35).*

PROOF. Let T be the polynomial ring $\mathbf{Z}[T_q, q : \text{prime}]$ of infinite variables. Define a surjective homomorphism $T \to \mathcal{T}_0(N)_{\mathbf{Z}}$ by $T_q \mapsto T_q$, and $T \to \mathcal{T}_0(M)_{\mathbf{Z}}[U]/(P_p(U))$ by $T_q \mapsto T_q$ $(q \neq p)$ and $T_p \mapsto U_p$. By Proposition 9.36, $\bigoplus_k s_k^* : \bigoplus_{k=0}^{e} J_0(M) \to J_0(N)$ is T-linear. By Corollary 9.30(2), the kernel of $\bigoplus_k s_k^* : \bigoplus_{k=0}^{e} J_0(M) \to J_0(Mp^e)$ is finite. Thus, the kernel of $T \to \mathcal{T}_0(N)_{\mathbf{Z}} \subset \operatorname{End} J_0(N)$ is contained in the kernel of $T \to \mathcal{T}_0(M)_{\mathbf{Z}}[U]/(P_p(U)) \subset \operatorname{End}(\bigoplus_{k=0}^{e} J_0(M))$. The assertion follows from this. ☐

Let $N = M\prod_{p\in S} p^{e_p}$, where $p \nmid M$ if $p \in S$. Applying Corollary 9.37 repeatedly, we obtain the ring homomorphism

$$\mathcal{T}_0(N)_{\mathbf{Z}} \longrightarrow \mathcal{T}_0(M)_{\mathbf{Z}}[U_p; p \in S]/(P_p(U_p); p \in S). \tag{9.36}$$

PROPOSITION 9.38. *Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p.*

1. *The action of the Hecke operator T_p on the cokernel $\operatorname{Coker}(s_0^* \oplus s_1^* : J_0(M)^2 \to J_0(Mp))$ equals -1 times the action of the Atkin–Lehner involution w_p and satisfies $T_p^2 = 1$.*
2. *Let $e \geq 2$ be an integer. The action of T_p^{e-1} on the cokernel $\operatorname{Coker}(\bigoplus_k s_k^* : J_0(Mp)^e \to J_0(Mp^e))$ equals 0.*

PROOF. (1) By Lemma 9.35(1) and (3), we have $T_p + w_p = s_{0*} \circ s_1^* + w_p = s_1^* \circ s_{0*}$. Thus, the image of $T_p + w_p$ is contained in the image of $s_0^* \oplus s_1^* : J_0(M)^2 \to J_0(Mp)$, and $T_p + w_p$ induces the 0 morphism on the cokernel $J = \operatorname{Coker}(s_0^* \oplus s_1^* : J_0(M)^2 \to J_0(Mp))$. Therefore, we have $T_p = -w_p$ as an endomorphism of J. Since $w_p^2 = 1$, we have $T_p^2 = 1$.

(2) By Lemma 9.35(1), we have $T_p = s_{1*} \circ s_0^*$. Thus, we have $T_p = s_0^* \circ s_{1*}$ by Lemma 9.35(2). Repeating this, we obtain $T_p^{e-1} = s_0^* \circ s_{e-1*}$. Hence, as in (1), T_p^{e-1} induces the 0 morphism on the cokernel $\operatorname{Coker}(\bigoplus_k s_k^* : J_0(Mp)^e \to J_0(Mp^e))$. □

COROLLARY 9.39. *Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p. Let K be a field of characteristic* 0.

(1) *If $f \in S_0(Mp)_K$ is a primitive form of level Mp, then we have $a_p(f) = \pm 1$.*
(2) *Let $e \geq 2$ be an integer. If $f \in S_0(Mp^e)_K$ is a primitive form of level Mp^e, then we have $a_p(f) = 0$.*

PROOF. Clear from Proposition 9.38. □

THEOREM 9.40. *Let $N \geq 1$ be an integer. For a primitive form $f \in \Phi(N)(\mathbf{C})$, we denote its level by $N_f \mid N$. Then, we have*

$$S_0(N)_{\mathbf{C}} = \bigoplus_{f \in \Phi(N)(\mathbf{C})} \bigoplus_{d \mid N/N_f} \mathbf{C} \cdot s_d^* f.$$

PROOF. For a primitive form $f \in \Phi(N)(\mathbf{C})$ of level $N_f | N$, we only show that $s_d^* f$ $(d | N/N_f)$ are linearly independent, and the other part of the proof is omitted.

Let $f = \sum_{n=1}^{\infty} a_n q^n \in \Phi(N)(\mathbf{C})$ be a primitive form of level $N_f | N$. Suppose there is a nontrivial relation $\sum_{d | N/N_f} c_d s_d^* f = 0$, and let d be the smallest integer $d \mid N/N_f$ such that $c_d \neq 0$. By (9.26), the coefficient of q^d is $dc_d a_1 = 0$. Since f is primitive, $a_1 = 1$, which is a contradiction. □

Let $N \geq 1$ be an integer, let K be a field of characteristic 0, and let f be a primitive form of level $N_f \mid N$ over K. For a prime number $p \mid N/N_f$, let $e_p = \operatorname{ord}_p N/N_f$, and define a polynomial $P_{f,p}(U_p) \in K_f[U_p]$ of degree $e_p + 1$ by

$$P_{f,p}(U_p) = \begin{cases} U_p^{e_p - 1}(U_p^2 - a_p(f)U_p + p) & \text{if } p \nmid N_f, \\ U_p^{e_p}(U_p - a_p(f)) & \text{if } \operatorname{ord}_p N_f = 1, \\ U_p^{e_p+1} & \text{if } p^2 | N_f. \end{cases} \tag{9.37}$$

By Corollary 9.39(2), $P_{f,p}(U_p)$ is the characteristic polynomial of the matrix U_p in Proposition 9.36 with T_p replaced by $a_p(f)$.

COROLLARY 9.41. *Let $N \geq 1$ be an integer, and let $\Phi(N)$ be the finite étale scheme over $\mathbf{Q}$ consisting of primitive forms of level dividing N, defined as $\operatorname{Spec} T_0'(N)_{\mathbf{Q}}$. For $f \in \Phi(N)$, let K_f be its* *residue field, and let* N_f *be the level of* f*. Then, we have* $T_0'(N)_{\mathbf{Q}} = \prod_{f\in\Phi(N)} K_f$*, and we obtain a ring homomorphism*

$$T_0(N)_{\mathbf{Q}} \longrightarrow \prod_{f\in\Phi(N)} K_f[U_p, p|N/N_f]/(P_{f,p}(U_p), p|N/N_f) \tag{9.38}$$

by defining the f *component of the image of* T_p *equal to* $a_p(f)$ *if* $p \nmid N/N_f$*, and* U_p *if* $p \mid N/N_f$*.*

PROOF. We have $T_0'(N)_{\mathbf{Q}} = \prod_{f\in\Phi(N)} K_f$ since $T_0'(N)_{\mathbf{Q}}$ is reduced. Therefore, we have $T_0(N)_{\mathbf{Q}} = \prod_{f\in\Phi(N)} T_0(N)_{\mathbf{Q}} \otimes_{T_0'(N)_{\mathbf{Q}}} K_f$. We define a ring isomorphism

$$K_f[U_p, p|N/N_f]/(P_{f,p}(U_p), p|N/N_f) \longrightarrow T_0(N)_K \otimes_{T_0(N)'_K} K_f. \tag{9.39}$$

For subrings $T_0'(N)[T_p : p\nmid N/N_f] \subset T_0(N)$ and $T_0'(N_f)[T_p : p\nmid N/N_f] \subset T_0(N_f)$, the natural surjection $T_0'(N) \to T_0'(N_f)$ induces an isomorphism $T_0'(N_f) \otimes_{T_0'(N)} [T_p : p \nmid N/N_f] \to T_0'(N_f)[T_p : p \nmid N/N_f]$. Thus, by Corollary 2.61, we obtain an isomorphism

$$K_f \otimes_{T_0'(N)_K} T_0'[T_p : p \nmid N/N_f] \to K_f.$$

Thus, we have

$$T_0(N)_K \otimes_{T_0(N)'_K} K_f = K_f[T_p, p|N/N_f] \subset \mathrm{End}(S_0(N)_{\mathbf{Q}} \otimes_{T_0'(N)_{\mathbf{Q}}} K_f).$$

Consider the polynomial ring $K_f[U_p, p|N/N_f]$, and define a surjection $K_f[U_p, p|N/N_f] \to T_0(N)_K \otimes_{T_0(N)'_K} K_f$ by $U_p \mapsto T_p$. We prove that its kernel is generated by $P_{f,p}(U_p)$ $(p|N/N_f)$. It suffices to show it after tensoring $\mathbf{C}$ over K_f.

We have $S_0(N)_{\mathbf{Q}} \otimes_{T_0'(N)_{\mathbf{Q}} \nearrow \varphi_f} \mathbf{C} = \bigoplus_{d|N/N_f} \mathbf{C} \cdot s_d^* f$ by Theorem 9.40. By Proposition 9.36, $\bigoplus_{d|N/N_f} \mathbf{C} \cdot s_d^* f$ is generated by $s_1^* f$ as a $\mathbf{C}[T_p, p|N/N_f]$-module. Moreover, $\bigoplus_{d|N/N_f} \mathbf{C} \cdot s_1^* f$ is a basis of the free $\mathbf{C}[U_p, p|N/N_f]/(P_{f,p}(U_p), p|N/N_f)$-module $\bigoplus_{d|N/N_f} \mathbf{C} \cdot s_d^* f$. Thus, we obtain the isomorphism (9.39). It is clear that the product of the inverse of (9.39) gives the isomorphism (9.38). □

COROLLARY 9.42. *Since* $g_0(11) = 1$ *and* $g_0(22) = 2$*, we have* $T_0(11)_{\mathbf{Z}} = \mathbf{Z}$ *and the surjection* $T_0(22)_{\mathbf{Z}} \to T_0(11)_{\mathbf{Z}}[U_2]/(U_2^2 - T_2U_2 + 2)$ *is an isomorphism. If* $f = \sum_{n=1}^{\infty} a_n(f) q^n$ *is the unique primitive form of level* 11*, we have* $a_2(f) = -2$*, and thus* $T_0(22)_{\mathbf{Z}} = \mathbf{Z}[U_2]/(U_2^2 + 2U_2 + 2)$ *is isomorphic to* $\mathbf{Z}[\sqrt{-1}]$ *by letting* $U_2 = -1 + \sqrt{-1}$.

9.6. Néron model of the Jacobian $J_0(Mp)$

In this section, p is a prime number, $M \geq 1$ is an integer relatively prime to p, and $N = Mp$. As a preparation of the proof of Theorem 3.55 in the next section, we study the mod p reduction $J_0(Mp)_{\mathbf{F}_p}$ of the Néron model of $J_0(Mp)$. By Theorem 8.63(3), $X_0(Mp)$ has semistable reduction at p, so does $J_0(Mp)$ by Corollary D.22. Thus, $J_0(Mp)_{\mathbf{F}_p}$ is a successive extension of the group Φ of the connected component, the abelian part $J_0(Mp)^{\mathrm{a}}_{\mathbf{F}_p}$, and the torus part $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$. In what follows, we denote the Hecke algebra $T_0(Mp)_{\mathbf{Z}}$ by $\boldsymbol{T}$. Φ, $J_0(Mp)^{\mathrm{a}}_{\mathbf{F}_p}$ and $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$ are naturally $\boldsymbol{T}$-modules.

The goal of this section is to prove Proposition 9.44, which is about the group Φ of connected components, and Proposition 9.45, which is about the character group $X = \mathrm{Hom}(J_0(Mp)^{\mathrm{t}}_{\bar{\mathbf{F}}_p}, \mathbf{G}_m)$ of the torus $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$. Let $\Gamma = [\Gamma_1 \to \Gamma_0]$ be the dual chain complex of $X_0(N)_{\mathbf{F}_p}$ (see Definition B.5). We identify the group Φ of connected components with $H^1(\Gamma^*)/\bar{\alpha}_1(H_1(\Gamma))$ by Corollary D.21(2). Also, by Corollary D.20, we identify the character group X with $H_1(\Gamma)$. First, we give a concrete description of the dual chain complex $\Gamma = [\Gamma_1 \to \Gamma_0]$.

By Theorem 8.63(3), we identify the reduced closed subscheme Σ of ordinary double points of $X_0(N)_{\mathbf{F}_p}$ with the reduced closed subscheme $X_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}$ of supersingular points of $X_0(M)_{\mathbf{F}_p}$. Moreover, we identify the normalization of $X_0(N)_{\mathbf{F}_p}$ with $X_0(M)_{\mathbf{F}_p} \amalg X_0(M)_{\mathbf{F}_p}$ through $(j_0, j_1) : X_0(M)_{\mathbf{F}_p} \amalg X_0(M)_{\mathbf{F}_p} \to X_0(N)_{\mathbf{F}_p}$, and $X_0(M)_{\bar{\mathbf{F}}_p}$ is connected. Thus, the set P of irreducible components of $X_0(N)_{\mathbf{F}_p}$ is identified with $\{0,1\}$, and the inverse image of Σ in $X_0(M)_{\mathbf{F}_p} \amalg X_0(M)_{\mathbf{F}_p}$ is identified with $\Sigma \times \{0,1\}$. Hence, Γ_0 is identified with $\mathbf{Z}^{\{0,1\}}$. Also, Γ_1 is identified with $\mathrm{Ker}(\mathbf{Z}^{\Sigma(\bar{\mathbf{F}}_p)\times\{0,1\}} \to \mathbf{Z}^{\Sigma(\bar{\mathbf{F}}_p)})$. Furthermore, by identifying $e_{x,0} - e_{x,1}$ with e_x for $x \in \Sigma(\bar{\mathbf{F}}_p)$, Γ_1 is identified with $\mathbf{Z}^{\Sigma(\bar{\mathbf{F}}_p)}$.

Γ_0 and Γ_1 naturally have structures of $\boldsymbol{T}$-modules, and the natural mapping $\Gamma_0 \to \Gamma_0$ that defines the dual chain complex Γ is a homomorphism of $\boldsymbol{T}$-modules. Let $\Gamma_0^* = \mathrm{Hom}(\Gamma_0, \mathbf{Z})$ and $\Gamma_1^* = \mathrm{Hom}(\Gamma_1, \mathbf{Z})$. These are also $\boldsymbol{T}$-modules, and the dual $\Gamma_0^* \to \Gamma_1^*$ is also a homomorphism of $\boldsymbol{T}$-modules. For $x = [(E, C)] \in \Sigma(\bar{\mathbf{F}}_p) = X_0(M)^{\mathrm{ss}}_{\mathbf{F}_p}(\bar{\mathbf{F}}_p)$, let $G_x = \mathrm{Aut}(E, C)/\{\pm 1\}$. The natural injection $\alpha_1 : \Gamma_1 \to \Gamma_1^*$ is defined by letting the image of the standard basis e_x be equal to $\sharp G_x$ times the dual basis e_x^*. $\bar{\alpha}_1 : H_1(\Gamma) \to H^1(\Gamma^*)$

is induced by $\alpha_1 : \Gamma_1 \to \Gamma_1^*$. These are also homomorphisms of $\boldsymbol{T}$-modules. We identify Γ_1 with a submodule of Γ_1^* through $\alpha_1 : \Gamma_1 \to \Gamma_1^*$. We denote $H_1(\Gamma) = \operatorname{Ker}(\Gamma_1 \to \Gamma_0)$ by Γ_1^0. By Corollary D.21(2), the group Φ of connected components is identified with $H^1(\Gamma^*)/\bar{\alpha}_1(H_1(\Gamma)) = \Gamma_1^*/(\Gamma_1^0 + \Gamma_0^*)$.

EXAMPLE 9.43. Let $p = N = 11$. By Example 8.65, the only supersingular points of $Y(1)_{\mathbf{F}_{11}}$ are $j = 0$ and 1, and their indices are 3 and 2, respectively. If we let $\Gamma_1 = \mathbf{Z}e_0 \oplus \mathbf{Z}e_1$, we have $H_1(\Gamma) = \Gamma_1^0 = \mathbf{Z}(e_0 - e_1)$. If we let $\Gamma_1^* = \mathbf{Z}e_0^* \oplus \mathbf{Z}e_1^*$, we have $\alpha_1 : \Gamma_1 \to \Gamma_1^*$, defined by $e_0 \mapsto 3e_0^*, e_1 \mapsto 2e_1^*$. We have $H^1(\Gamma^*) = \mathbf{Z}\bar{e}_0^*$ and $\bar{e}_1^* = -\bar{e}_0^*$. Thus, $\bar{\alpha}_1 : H_1(\Gamma) \to H^1(\Gamma^*)$ sends a basis $e_0 - e_1$ of $H_1(\Gamma)$ to $5\bar{e}_0^*$. Thus, in this case we have $\Phi \simeq \mathbf{Z}/5\mathbf{Z}$.

PROPOSITION 9.44. *If r is a prime number relatively prime to Mp, the Hecke operator T_r acts on the $\boldsymbol{T}$-module Φ as the multiplication by $r + 1$.*

PROOF. Let $\Gamma = [\Gamma_1 \to \Gamma_0]$ be the dual chain complex of $X_0(N)_{\mathbf{F}_p}$. We identify the group of connected components Φ with

$$\Phi = H^1(\Gamma^*)/\bar{\alpha}_1(H_1(\Gamma)) = \Gamma_1^*/(\Gamma_1^0 + \Gamma_0^*).$$

Consider the diagram of $\boldsymbol{T}$-modules

$$\begin{tikzcd}
0 \arrow[r] & \Gamma_1/\Gamma_1^0 \arrow[r] \arrow[d, "\cap"'] & \Gamma_1^*/\Gamma_1^0 \arrow[r] \arrow[d] & \Gamma_1^*/\Gamma_1 \arrow[r] & 0 \\
 & \Gamma_0 & \Gamma_1^*/(\Gamma_1^0 + \Gamma_0^*) = \Phi. & &
\end{tikzcd} \tag{9.40}$$

The upper row is exact. Define an ideal J of $\boldsymbol{T}$ by

$$J = (T_r - (r+1); r \text{ is relatively prime to } Mp).$$

We now show that all the $\boldsymbol{T}$-modules in (9.40) are annihilated by J. If r is a prime number relatively prime to Mp, then T_r acts on $\Gamma_0 = \mathbf{Z}^{\{0,1\}}$ by the multiplication by $r + 1$, and thus $J \cdot \Gamma_0 = 0$. Since $\Gamma_1/\Gamma_1^0 \to \Gamma_0$ is injective, we have $J \cdot \Gamma_1/\Gamma_1^0 = 0$.

Next we show $J \cdot \Gamma_1^*/\Gamma_1 = 0$. Let r be a prime number relatively prime to Mp. It suffices to show $(T_r - (r+1))e_y^* \in \Gamma_1$ for each $y \in \Sigma(\bar{\mathbf{F}}_p)$. In other words, it suffices to show that $((T_r - (r+1))e_y^*)(e_x) = e_y^*((T_r - (r+1)) \cdot e_x)$ is divisible by $\sharp G_x$ for each $x, y \in \Sigma(\bar{\mathbf{F}}_p)$. If $x = [(E, C)]$, we have $T_r e_x = \sum_{H \subset E}[(E/H, C + H/H)]$, where H

runs all the subgroups of E of order r. Since

$$\sum_{y \in \Sigma(\bar{\mathbf{F}}_p)} e_y^*((T_r - (r+1)) \cdot e_x) = 0,$$

it suffices to show that $e_y^*((T_r - (r+1)) \cdot e_x) = e_y^*(T_r \cdot e_x)$ is divisible by $\sharp G_x$ for $x \neq y$. If $x = [(E, C)] \neq y = [(E', C')]$, then $e_y^*(T_r \cdot e_x)$ is the number of elements of the set

$$I_{x,y} = \left\{ H \subset E \;\middle|\; \begin{array}{l} H \text{ is a subgroup of } E \text{ of order } r \text{ such that} \\ (E/H, C + H/H) \text{ is isomorphic to } (E', C') \end{array} \right\}.$$

Thus, it suffices to show the natural action of $G_x = \mathrm{Aut}(E, C)/\{\pm 1\}$ on $I_{x,y}$ is a free action.

We show that the action of G_x on $I_{x,y}$ is a free action. Suppose $\alpha \neq \pm 1 \in \mathrm{Aut}(E, C)$ and $H \in I_{x,y}$ satisfy $\alpha(H) = H$. Then, by Lemma 8.41(1), $\alpha \in \mathrm{End}(E, C)$ satisfies one of the relations $\alpha^2 + 1 = 0$, $\alpha^2 + \alpha + 1 = 0$ and $\alpha^2 - \alpha + 1 = 0$, and the subring $\mathbf{Z}[\alpha] \subset \mathrm{End}(E, C)$ is isomorphic to either $\mathbf{Z}[\sqrt{-1}]$ or $\mathbf{Z}[\frac{-1+\sqrt{-3}}{2}]$. Moreover, the group $E[r]$ of r-torsion points of E is a free $\mathbf{Z}[\alpha]/(r)$-module of rank 1 and H is a submodule of order r. Thus, if such an H exists, r is decomposed to the product $r = \pi\pi'$ of prime elements in the principal ideal domain $\mathbf{Z}[\alpha]$, and we have $H = \mathrm{Ker}(\pi : E \to E)$. In this case, the multiplication by π induces the isomorphism $(E/H, C + H/H) \to (E, C)$, and it contradicts the assumption. Hence, we proved the action of G_x on $I_{x,y}$ is a free action. Thus, we proved $J \cdot \Gamma_1^*/\Gamma_1 = 0$.

We now prove $J \cdot \Gamma_1^*/\Gamma_1^0 = 0$. Since $J \cdot \Gamma_1^*/\Gamma_1 = 0$, $J \cdot \Gamma_1^*/\Gamma_1^0$ is a subgroup of Γ_1/Γ_1^0. By Lemma 8.41, the order of $G_x = \mathrm{Aut}(E, C)/\{\pm 1\}$ is a divisor of 12 for each $x \in \Sigma$. Thus, Γ_1^*/Γ_1 is a finite abelian group, and $12 \cdot \Gamma_1^*/\Gamma_1 = 0$. Thus, we have $12\Gamma_1^*/\Gamma_1^0 \subset \Gamma_1/\Gamma_1^0$, and $12J \cdot \Gamma_1^*/\Gamma_1^0 \subset J\Gamma_1/\Gamma_1^0 = 0$. Thus, $J \cdot \Gamma_1^*/\Gamma_1^0$ is a subgroup of $\Gamma_1/\Gamma_1^0 \subset \Gamma_0 = \mathbf{Z}^{\{0,1\}}$ that becomes 0 after multiplying by 12, which implies $J \cdot \Gamma_1^*/\Gamma_1^0 = 0$. Since the vertical arrow $\Gamma_1^*/\Gamma_1^0 \to \Phi$ in (9.40) is surjective, we conclude $J \cdot \Phi = 0$. □

PROPOSITION 9.45. *The action of the Frobenius substitution* $\varphi_p \in G_{\mathbf{F}_p}$ *on the character group* $X = \mathrm{Hom}(J_0(Mp)^{\mathrm{t}}_{\bar{\mathbf{F}}_p}, \mathbf{G}_m)$ *of* $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$ *equals the action of the Hecke operators* T_p, *and* $\varphi_p^2 = 1$ *holds.*

PROOF. Since the Atkin–Lehner involution w_p satisfies $w_p^2 = 1$, it suffices to show $\varphi_p = -w_p$ by Proposition 9.38. The action of the Frobenius substitution φ_p on X equals the action of the Frobenius endomorphism F. By Corollary D.20, X is identified with $H_1(\Gamma) \subset$

$\Gamma_1 = \mathrm{Ker}(\mathbf{Z}^{\Sigma(\bar{\mathbf{F}}_p)\times\{0,1\}} \to \mathbf{Z}^{\Sigma(\bar{\mathbf{F}}_p)})$. Thus, it suffices to compare the actions of the Atkin–Lehner involution w_p and the Frobenius homomorphism on $\Sigma(\bar{\mathbf{F}}_p) \times \{0,1\}$.

Let (E, C, C') be a supersingular point of $X_0(Mp)_{\mathbf{F}_p}$. Since $C' = \mathrm{Ker}\ F$, the action of the Atkin–Lehner involution w_p is given by $w_p(E, C, \mathrm{Ker}\ F) = (E^{(p)}, C^{(p)}, \mathrm{Ker}\ F)$. Thus, the action of w_p on the set $\Sigma(\bar{\mathbf{F}}_p)$ of supersingular points equals the action of F. Moreover, w_p permutes irreducible components of $X_0(Mp)_{\mathbf{F}_p}$, and F preserves irreducible components. Hence, the action of w_p on $X \subset \Gamma_1$ coincides with that of $-F$. ☐

COROLLARY 9.46. *Let p be a prime number, let $M \geq 1$ be an integer relatively prime to p, let $e \geq 1$ be an integer, and let $N = Mp^e$. If $\ell \neq p$ is a prime number, then the action of the Frobenius substitution φ_p on the cokernel* $\mathrm{Coker}(\bigoplus_k s_k^* : \bigoplus_{k=0}^{e-1} V_\ell J_0(M) \to V_\ell J_0(N)^{I_p})$ *is the multiplication of pT_p, and its eigenvalue is $\pm p$.*

PROOF. The morphism $\bigoplus t_k^*$ induces a surjection $V_\ell J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p} \to \mathrm{Coker}(\bigoplus_k s_k^* : \bigoplus_{k=0}^{e-1} V_\ell J_0(M) \to V_\ell J_0(N)^{I_p})$ by Corollary 9.30(1). If X is the character group of the torus $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$, then $V_\ell J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$ is isomorphic to $\mathrm{Hom}(X, \mathbf{Q}_\ell(1))$. Thus, by Proposition 9.45, the action of the Frobenius substitution φ_p on $V_\ell J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$ is the multiplication by pT_p, and its eigenvalue is $\pm p$. ☐

From Proposition 9.45, we have the following proposition on the properties of ℓ-adic representations associated with modular forms.

PROPOSITION 9.47. *Let p be a prime number, let $M \geq 1$ be an integer relatively prime to p, and let $N = Mp$. Let ℓ be a prime number, and let $\mathcal{O}$ be the ring of integer of a finite extension K of $\mathbf{Q}_\ell$. Let $f \in S_0(N)_K$ be a primary form of level N with K coefficients. Suppose the ℓ-adic representation V_f of $G_{\mathbf{Q}}$ associated with f is bad at p. Then, V_f is ordinary at p. The coinvariant quotient V_{f,I_p} of the restriction of V_f to the decomposition group $G_{\mathbf{Q}_p}$ by the inertia I_p defines a one-dimensional representation of $G_{\mathbf{F}_p}$, and the action of the Frobenius substitution $\varphi_p \in G_{\mathbf{F}_p}$ on V_{f,I_p} is the multiplication by $a_p(f) = \pm 1$.*

PROOF. Since $p^2 \nmid N$, the ℓ-adic representation V_f is semistable at p by Theorem 3.52(2) (ii) $\Rightarrow$ (i). Since V_f is bad at p, V_f is ordinary at p. By Corollary 9.19, We may assume V_f is a subrepresentation of $V_\ell J_1(N) \otimes_{\mathbf{Q}_\ell} K$. Moreover, since V_f is not good at p, it is not modular of level M and is a subrepresentation of

$$\operatorname{Coker}(s^* \oplus t^* : V_\ell J_0(M)^{\oplus 2} \to V_\ell J_0(N)) \otimes_{\mathbf{Q}_\ell} K$$

by Theorem 3.52(1)(ii) $\Rightarrow$ (i).

We deal with the case $p \neq \ell$. The case $p = \ell$ is similar, and we omit it. Since V_f is ordinary and it is not unramified, the I_p invariant part $V_f^{I_p} \subset V_f$ is one dimensional, and the coinvariant quotient V_{f,I_p} equals $V_f/V_f^{I_p}$. We have

$$V_f^{I_p} = V_f \cap \operatorname{Coker}(s^* \oplus t^* : V_\ell J_0(M)^{\oplus 2} \to V_\ell J_0(N)^{I_p}) \otimes_{\mathbf{Q}_\ell} K.$$

By Corollary 9.46, the action of φ_p on $\operatorname{Coker}(s^* \oplus t^* : V_\ell J_0(M)^{\oplus 2} \to V_\ell J_0(N)^{I_p})$ is the multiplication by pT_p. Thus, its action on $V_f^{I_p}$ is the multiplication by $a_p(f)p = \pm p$. The action of $G_{\mathbf{Q}_p}$ on $V_f/V_f^{I_p}$ is also unramified, and $\det(\varphi_p : V_f) = p$. Thus, the action of φ_p on $V_f/V_f^{I_p}$ is the multiplication by $a_p(f) = \pm 1$. ☐

COROLLARY 9.48. *Let ℓ be an odd prime number, and let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$. Let p a prime number, and let $N = Mp$, $p \nmid M$. Let $\bar\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be a modular* mod *ℓ representation of level N.*

(1) *Suppose $\bar\rho$ is not good at p. Then $\bar\rho$ is ordinary at p. The coinvariant quotient $\bar\rho_{I_p}$ by the inertia group I_p defines a character of $G_{\mathbf{F}_p}$, and we have*

$$\bar\rho_{I_p}(\varphi_p) = \bar\varphi(T_p) = \pm 1$$

for the Frobenius substitution φ_p.

(2) *Let K be a finite extension of $\mathbf{Q}_\ell$, and let $f \in S_0(N)_K$ be a primitive form of level N. Let $\mathbf{F}$ be a finite extension of the residue field of K, and suppose $\operatorname{Tr}(\varphi_q) \equiv a_q(f)$ for almost all $q \nmid N\ell$. Then, $\bar\rho$ is ordinary at p. Furthermore, suppose $p = \ell$ and $\bar\rho$ is good at $p = \ell$. Let $D(\bar\rho)$ be the F-module obtained by applying Theorem* C.6 *to the restriction of $\bar\rho$ to $G_{\mathbf{Q}_\ell}$. Then, we have*

$$\operatorname{Tr}(F : D(\bar\rho)) = \bar\rho_{I_p}(\varphi_p) \equiv a_p(f).$$

PROOF. (1) Let K be a finite extension of $\mathbf{Q}_\ell$, and let $f \in S_0(N)_K$ be a primary form of level N satisfying $\rho_f \equiv \bar\rho$. If $\bar\rho$ is not good at p, then neither is ρ_f. By Proposition 9.47, ρ_f is ordinary, and thus so is $\bar\rho$. Since the coinvariant quotient $\bar\rho_{I_p}$ is not the entire space, it is one dimensional and $\rho_{f,I_p} \equiv \bar{\rho}_{I_p}$. The assertion now follows from Proposition 9.47.

(2) Since the ℓ-adic representation V_f is semistable but not good at p, it is ordinary by Theorem 3.52. Thus, $\bar{\rho}$ is also ordinary.

Suppose $p = \ell$ and $\bar{\rho}$ is good at $p = \ell$. Since $\det \bar{\rho}$ is the mod ℓ cyclotomic character χ, the restriction of $\bar{\rho}$ to $G_{\mathbf{Q}_p}$ is the extension of the unramified character $\bar{\rho}_{I_p}$ by $\chi \cdot \bar{\rho}_{I_p}^{-1}$. Thus, the $\mathbf{F}[F, V]$-module $D\bar{\rho}$ is an extension of an $\mathbf{F}[F, V]$-module on which F acts as the multiplication by $\bar{\rho}_{I_p}(\varphi_p)$ by an $\mathbf{F}[F, V]$-module on which F acts as the multiplication by $p \cdot \bar{\rho}_{I_p}(\varphi_p)^{-1} = 0$. This shows the equality. The congruence relation is clear from Proposition 9.47. □

9.7. Level of modular forms and ramification of mod ℓ representations

In §3.8 in Chapter 3, we stated the following theorem of the level of modular forms and the ramification of mod ℓ representations.

THEOREM 3.55. *Let ℓ be an odd prime, let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$ and let $\bar{\rho} : G_{\mathbf{Q}} :\to \mathrm{GL}_2(\mathbf{F})$ be an irreducible continuous representation. Suppose $\bar{\rho}$ is modular of level N, and M is the prime to p part of N. Then, the following conditions* (i) *and* (ii) *in each of* (1) *and* (2) *are equivalent.*

(1) (i) *$\bar{\rho}$ is modular of level M.*
  (ii) *$\bar{\rho}$ is good at p.*

(2) (i) *$\bar{\rho}$ is modular of level pM.*
  (ii) *$\bar{\rho}$ is semistable at p.*

PROOF OF (i) ⇒ (ii). Similar to the proof of Theorem 3.52 (i) ⇒ (ii). □

In this book we do not prove Theorem 3.55(2) (ii) ⇒ (i). We prove (1) (ii) ⇒ (i) in the case $p \not\equiv 1 \bmod \ell$, assuming (2) (ii) ⇒ (i). In other words, we prove the following theorem in the case $p \not\equiv 1 \bmod \ell$.

THEOREM 9.49. *Let ℓ be an odd prime number, and let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$. Let p be a prime number, and let $M \geq 1$ be an integer relatively prime to p. Suppose $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ is a modular irreducible continuous representation of level $N = Mp$. Then, if $\bar{\rho}$ is good at p, $\bar{\rho}$ is modular of level M.*

In this book we give a proof of Theorem 9.49 only in the case $p \not\equiv 1$. In this case the proof uses results of §9.6, which are derived from Theorem 8.63(3) on the structure of the modular curve $X_0(Mp)$. We regret we are unable to include the proof of the case $p \equiv 1$ in this book because it requires more preparation.

For the proof of Theorem 9.49, we introduce notation for Hecke algebras. Define

$$(9.41) \qquad \boldsymbol{T} = T_0(Mp)_{\mathbf{Z}}, \qquad \boldsymbol{T}' = T_0(M)_{\mathbf{Z}}[U_p]/(U_p^2 - T_pU_p + p).$$

The natural surjection $\boldsymbol{T} \to \boldsymbol{T}'$ (9.35) which was defined in Corollary 9.37 is compatible with

$$(9.42) \qquad (s^*, t^*) : J_0(M) \times J_0(M) \longrightarrow J_0(N).$$

We give a sufficient condition for a mod ℓ representation to be modular of level M in terms of the ring homomorphism $\boldsymbol{T} \to \boldsymbol{T}'$.

LEMMA 9.50. *Let $\bar\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be a modular absolutely irreducible continuous representation of lever Mp, and let $\bar\varphi : \boldsymbol{T} \to \mathbf{F}$ be a ring homomorphism satisfying*

$$\det(1 - \bar\rho(\varphi_q)t) = 1 - \bar\varphi(T_q)t + qt^2$$

for almost all prime numbers q. If there exist a finite extension $\mathbf{F}'$ of $\mathbf{F}$ and a ring homomorphism $\bar\varphi' : \boldsymbol{T}' \to \mathbf{F}'$ that makes the diagram

$$\begin{tikzcd} \boldsymbol{T} \arrow[r, "\bar\varphi"] \arrow[d] & \mathbf{F} \arrow[d] \\ \boldsymbol{T}' \arrow[r, "\bar\varphi'"] & \mathbf{F}' \end{tikzcd}$$

commutative, then $\bar\rho$ is modular of level M.

PROOF. Clear from Lemma 9.22 (ii) $\Rightarrow$ (i). □

PROOF OF THEOREM 9.49 IN THE CASE $p \not\equiv 1$. Let $\bar\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be a mod ℓ representation that satisfies the assumption of Theorem 9.49. Replacing $\mathbf{F}$ by its finite extension if necessary, take a ring homomorphism $\bar\varphi : \boldsymbol{T} = T_0(N)_{\mathbf{Z}} \to \mathbf{F}$ corresponding to $\bar\rho$ by Lemma 9.22. Let $\mathfrak{m}$ be the maximal ideal of $\boldsymbol{T}$ that is the kernel of $\bar\varphi : \boldsymbol{T} \to \mathbf{F}$. Let $J_0(Mp)[\mathfrak{m}] = \{x \in J_0(Mp)(\bar{\mathbf{Q}}) \mid ax = 0 \text{ for all } a \in \mathfrak{m}\}$. $J_0(Mp)[\mathfrak{m}]$ defines a mod ℓ representation of $G_{\mathbf{Q}}$. The finite étale group scheme over $\mathbf{Q}$ corresponding to the mod ℓ representation $J_0(Mp)[\mathfrak{m}]$ is also denoted by $J_0(Mp)[\mathfrak{m}]$.

By Lemma 9.28, $J_0(Mp)[\mathfrak{m}]$ is nonzero, and $J_0(Mp)[\mathfrak{m}] \otimes_{\boldsymbol{T}} \mathbf{F}$ is isomorphic to the direct sum of copies of $\bar\rho$ as a mod ℓ representation of $G_{\mathbf{Q}}$. By assumption, $\bar\rho$ is good at p, and the finite étale group scheme $J_0(Mp)[\mathfrak{m}]_{\mathbf{Q}_p}$ over $\mathbf{Q}_p$ extends to a finite étale group scheme $J_0(Mp)[\mathfrak{m}]_{\mathbf{Z}_p}$ over $\mathbf{Z}_p$. If $p \neq \ell$, then $J_0(Mp)[\mathfrak{m}]_{\mathbf{Z}_p}$ is finite étale, the inclusion $J_0(Mp)[\mathfrak{m}] \to J_0(Mp)$ extends to a morphism $J_0(Mp)[\mathfrak{m}]_{\mathbf{Z}_p} \to J_0(Mp)_{\mathbf{Z}_p}$ over $\mathbf{Z}_p$ by the properties of Néron models. By Proposition D.12(2), this is a closed immersion. In the case $p = \ell$ also, the inclusion $J_0(Mp)[\mathfrak{m}] \to J_0(Mp)$ extends to a closed immersion $J_0(Mp)[\mathfrak{m}]_{\mathbf{Z}_p} \to J_0(Mp)_{\mathbf{Z}_p}$. Taking the reduction mod p, we obtain a closed immersion $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to J_0(Mp)_{\mathbf{F}_p}$ over $\mathbf{F}_p$.

Here, $J_0(Mp)_{\mathbf{F}_p}$ denotes the reduction mod p of the Néron model of $J_0(Mp)$. Let Φ be the group of connected components of $J_0(Mp)_{\mathbf{F}_p}$, let $J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p}$ be the abelian part, and let $J_0(Mp)^{\mathfrak{t}}_{\mathbf{F}_p}$ be the torus part. The $\boldsymbol{T}$-module scheme $J_0(Mp)_{\mathbf{F}_p}$ over $\mathbf{F}_p$ is a successive extension of three $\boldsymbol{T}$-module schemes

$$\Phi, \quad J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p}, \quad J_0(Mp)^{\mathfrak{t}}_{\mathbf{F}_p}.$$

Using this fact, we prove the theorem in the following order.

(1) Show that the composition $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to J_0(Mp)_{\mathbf{F}_p} \to \Phi$ is the 0 morphism using Proposition 9.44 and Lemma 9.28(3).

(2) By (1) a morphism $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p}$ is induced. If this is not the 0 morphism, show that $\bar{\rho}$ is modular of level M using Lemma 9.50.

(3) If $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p}$ is 0 morphism, show that $p \equiv 1 \bmod \ell$ using Proposition 9.45 and Lemma 9.28(1), (2).

(1) We show that the composition $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to \Phi$ is the 0 morphism. $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p}$ is a $\boldsymbol{T}/\mathfrak{m}$-module. If we define an ideal J' of $\boldsymbol{T}$ by $J' = (T_r - (r+1); r \nmid Mp\ell)$, then Φ is a $\boldsymbol{T}/J'$-module by Proposition 9.44.

We show $\boldsymbol{T} = \mathfrak{m} + J'$. Since $\mathfrak{m}$ is a maximal ideal, if $\boldsymbol{T} = \mathfrak{m} + J'$ does not hold, we have $J' \subset \mathfrak{m}$. If $\bar{\chi} : (\mathbf{Z}/\ell\mathbf{Z})^\times \to \mathbf{F}^\times$ is the mod ℓ cyclotomic character, we have $T_r \equiv r + 1 = \bar{\chi}(r) + 1 \bmod \mathfrak{m}$ for all prime numbers $r \nmid Mp\ell$. This implies $\mathfrak{m}$ is an Eisenstein ideal, which contradicts Proposition 9.26.

(2) We show $J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p}$ is a $\boldsymbol{T}'$-module. By Theorem 8.63(3), $(j_0^*, j_1^*) : J_0(Mp)_{\mathbf{F}_p} \to J_0(M)_{\mathbf{F}_p} \times J_0(M)_{\mathbf{F}_p}$ induces an isomorphism $J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p} \to J_0(M)_{\mathbf{F}_p} \times J_0(M)_{\mathbf{F}_p}$. Since

$$(s^*, t^*) : J_0(M)_{\mathbf{F}_p} \times J_0(M)_{\mathbf{F}_p} \to J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p}$$

is an isogeny by Corollary 9.30(2), the $\boldsymbol{T}$-module $J_0(Mp)^{\mathfrak{a}}_{\mathbf{F}_p}$ is a $\boldsymbol{T}'$-module.

By (1), a morphism $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to J_0(Mp)^{\mathrm{a}}_{\mathbf{F}_p}$ is induced. The $\mathfrak{m}$-torsion part $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p}$ is a $\boldsymbol{T}/\mathfrak{m}$-module, and $J_0(Mp)^{\mathrm{a}}_{\mathbf{F}_p}$ is a $\boldsymbol{T}'$-module. Thus, if the morphism above is not the 0-morphism, $\boldsymbol{T}/\mathfrak{m}$ is a quotient of $\boldsymbol{T}'$ since $\mathfrak{m}$ is a maximal ideal. In this case $\bar{\rho}$ is modular of level M.

(3) If $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to J_0(Mp)^{\mathrm{a}}_{\mathbf{F}_p}$ is the 0 morphism, a morphism $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} \to J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$ is induced and we have $J_0(Mp)[\mathfrak{m}]_{\mathbf{F}_p} = J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}[\mathfrak{m}]$. If X is the character group of the torus $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}$, we have $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}[\mathfrak{m}] = \mathrm{Hom}(X/\mathfrak{m}X, \mu_\ell)$. Thus, we obtain an isomorphism $J_0(Mp)^{\mathrm{t}}_{\mathbf{F}_p}[\mathfrak{m}] = \mathrm{Hom}(X/\mathfrak{m}X, \mu_\ell)$ of a finite flat commutative group scheme over $\mathbf{Z}_p$.

We first show the case $p \neq \ell$. By Proposition 9.45 the action of the Frobenius substitution φ_p on $J_0(Mp)[\mathfrak{m}]$ is the multiplication by $\pm p$. By Lemma 9.28, $J_0(Mp)[\mathfrak{m}] \otimes_{\boldsymbol{T}} \mathbf{F}$ is not 0 and is isomorphic to the direct product of copies of $\bar{\rho}$. Thus, $\bar{\rho}(\varphi_p)$ is also the multiplication by $\pm p$, and $\det \bar{\rho}(\varphi_p) = p^2$. On the other hand, since we have $\det \bar{\rho}(\varphi_p) = p$, we have $p^2 = p \bmod \ell$, which implies $p \equiv 1 \bmod \ell$.

Assuming $p = \ell$, we derive a contradiction. Let $\alpha : G_{\mathbf{Q}_p} \to \mathbf{F}^\times$ be an unramified character defined by $\alpha(\varphi_p) \equiv (T_p \bmod \mathfrak{m}) = \pm 1$, and χ the mod p cyclotomic character. By Proposition 9.45, the action of $G_{\mathbf{Q}_p}$ on $J_0(Mp)[\mathfrak{m}]$ is the product of $\alpha^{-1} = \alpha$ and χ. Thus, as in the case $p \neq \ell$, the restriction of $\bar{\rho}$ to $G_{\mathbf{Q}_p}$ is also $(\alpha \cdot \chi)^{\oplus 2}$ and $\det \bar{\rho} = (\alpha \cdot \chi)^2 = \chi^2$. On the other hand, since we have $\det \bar{\rho} = \chi$, we obtain $\chi = 1$, which is a contradiction. □

We state one consequence of Theorem 3.55.

LEMMA 9.51. *Let ℓ be an odd prime number, and let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$. Let $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ be a modular semistable absolutely irreducible representation. If L is the quadratic subfield $\mathbf{Q}(\sqrt{(-1)^{\frac{\ell-1}{2}}\ell})$ of $\mathbf{Q}(\zeta_\ell)$, then the restriction $\bar{\rho}|_{G_L}$ is absolutely irreducible.*

PROOF. We prove it by contradiction. Suppose the restriction $\bar{\rho}|_{G_L}$ is absolutely reducible. Then, there exists a character $\chi : G_L \to \overline{\mathbf{F}}_\ell^\times$ such that $\bar{\rho} \simeq \mathrm{Ind}_{G_L}^{G_{\mathbf{Q}}} \chi$. Thus, the order of the image $\mathrm{Im}\, \bar{\rho}$ is relatively prime to ℓ. Since $\bar{\rho}$ is semistable, it is unramified at all primes except ℓ. If it is ordinary at ℓ, the restriction $\bar{\rho}|_{I_\ell}$ is the direct sum of the trivial character and the cyclotomic character. Thus, $\bar{\rho}$ is good at all primes. Hence, by Theorem 3.55, $\bar{\rho}$ is modular of level 1.

However, there is no modular form of level 1 and weight 2 other than 0. This is a contradiction. ☐

COROLLARY 9.52. *Let $\bar{\rho}$ be a semistable absolutely irreducible representation. If $n \geq 1$ is an integer, then the restriction $\bar{\rho}|_{G_{\mathbf{Q}(\zeta_{\ell^n})}}$ is absolutely irreducible.*

PROOF. We prove it by contradiction. If $\bar{\rho}|_{G_{\mathbf{Q}(\zeta_{\ell^n})}}$ is not absolutely irreducible, $\bar{\rho}|_{G_{\mathbf{Q}(\zeta_{\ell^n})}}$ is a direct sum of the characters χ and χ', and χ and χ' are conjugate under the action of $\mathrm{Gal}(\mathbf{Q}(\zeta_{\ell^n})/\mathbf{Q})$. Taking L as in Lemma 9.51, the character χ is invariant under the action of $\mathrm{Gal}(\mathbf{Q}(\zeta_{\ell^n})/\mathbf{Q})$ and defines a stable subspace of the restriction $\bar{\rho}|_{G_L}$. This contradicts Lemma 9.51. ☐

CHAPTER 10

Hecke modules

As we announced in Chapter 5, we will define Hecke modules as the completion of singular homology groups of modular curves. Then, we show that the families of liftings and *RTM*-triples satisfy the conditions of two theorems we proved in Chapter 6. In Chapter 5, we stated Proposition 5.30, which is about the surjectivity of morphisms of Hecke modules, Theorem 5.32(2), which says Hecke algebras are free modules over group rings, and Proposition 5.33, which is about the multiplier of the surjection of *RTM*-triples. These propositions will be proved as Propositions 10.11, 10.37, and 10.14. The main result of Chapter 5 that says the deformation ring R coincides with the Hecke algebra T (Theorem 5.22) will thus become a consequence of the computations of Selmer groups in the following chapter.

We will first define full Hecke algebras and Hecke modules in §10.1 and §10.2, respectively, and we will construct *RTM*-triples. We then compute the multiplier of a surjection of *RTM*-triples constructed out of Hecke modules in Proposition 10.14 in §10.2. The proof of Proposition 10.11 on the surjectivity of the morphism of *RTM*-triples defined in §10.2 will be given in §10.3. In §10.4, we will study the relation between the deformation ring and the group ring that is defined from a set of prime numbers satisfying certain conditions. In §10.5, we will define another kind of full Hecke algebras and Hecke modules, and construct a family of liftings. The fact that these Hecke modules define a family of liftings follows from Proposition 10.37. The proof of Proposition 10.37 will be given in §10.6. In §10.7, we put these results together, and reduce the proof of Theorem 5.22 to Theorems 5.32(1) and 5.34, which concern Selmer groups and will be proved in Chapter 11.

The properties of Hecke algebras presented in this chapter mainly follow from the properties of Hecke algebras with $\mathbf{Q}$ coefficients, and are proved using the ramification of Galois representations associated with modular forms and properties of old forms. On the other hand, the properties of Hecke modules depend essentially on the fact that the coefficients are in $\mathbf{Z}$, and these are proved by topological properties of modular curves and the fact that some maximal ideals are non-Eisenstein. The proof of the main result is given by combining these elements in an appropriate way.

10.1. Full Hecke algebras

We review briefly the notation we used in Chapter 5. Throughout this chapter ℓ is an odd prime number, and K is a finite extension of $\mathbf{Q}_\ell$. We denote by $\mathcal{O}$ its ring of integers and by $\mathbf{F}$ the residue field. $\bar{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F})$ is an irreducible modular semistable ℓ-adic representation, and $S_{\bar{\rho}}$ is the set of prime numbers p at which ρ is not good. By Corollary 3.56, $\bar{\rho}$ is modular with level $N_{\bar{\rho}} = N_\varnothing = \prod_{p \in S_{\bar{\rho}}} p$.

Let Σ be a finite set of prime numbers such that $S_{\bar{\rho}} \cap \Sigma = \varnothing$. In Chapter 5 we defined the deformation ring R_Σ, a positive integer $N_\Sigma = N_\varnothing \cdot \prod_{p \in \Sigma, p \neq \ell} p^2 \cdot \prod_{p \in \Sigma, p = \ell} p$, the set of primitive forms $\Phi(N_\Sigma)_{K,\bar{\rho}} \subset \Phi(N_\Sigma)_K$, the Hecke algebra T_Σ, and the surjective ring homomorphism $f_\Sigma : R_\Sigma \to T_\Sigma$. Definition 5.13 states that a primitive form $f \in \Phi(N_\Sigma)_K$ satisfies $f \in \Phi(N_\Sigma)_{K,\bar{\rho}}$ if and only if $T_p \equiv \operatorname{Tr} \bar{\rho}(\varphi_p) \bmod \mathfrak{m}_f$ for any prime number $p \nmid N_\Sigma \ell$. Here, $\mathfrak{m}_f$ is the maximal ideal of the valuation ring K_f. We have $T_\Sigma \otimes_{\mathcal{O}} K = T_{\Sigma,K} = \prod_{f \in \Phi(N_\Sigma)_{K,\bar{\rho}}} K_f$.

Let $\overline{V} = \mathbf{F}^2$ be the representation space of $\bar{\rho}$. If $\bar{\rho}$ is good at $p = \ell$, the restriction of $\overline{V}$ to $G_{\mathbf{Q}_p}$ defines an $\mathbf{F}[F, V]$-module $D(\overline{V})$ by Theorem C.1. Regard the action of F on $D(\overline{V})$ as a representation of F, and denote it by $D(\bar{\rho})$. By Corollary 9.23(2), we have $\operatorname{Tr}(F : D(\bar{\rho})) = \overline{\varphi}(T_\ell)$.

In this section, we denote the Hecke algebra $T_0(N)_{\mathbf{Z}}$ simply by $T(N)_{\mathbf{Z}}$. We define the full Hecke algebra $T_\Sigma^\flat$ as the completion of the Hecke algebra $T(N_\Sigma)_{\mathcal{O}} = T(N_\Sigma)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathcal{O}$ at some maximal ideal. We first find the maximal ideal at which we take the completion.

Proposition 10.1. *There exists a unique $\mathcal{O}$-algebra homomorphism $\overline{\varphi}_\Sigma : T(N_\Sigma)_{\mathcal{O}} = T(N_\Sigma)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathcal{O} \to \mathbf{F}$ satisfying the following* *condition*:

$$\overline{\varphi}_\Sigma(T_p) = \begin{cases} \operatorname{Tr} \bar{\rho}(\varphi_p) & \textit{if } p \neq \ell, \notin S_{\bar{\rho}} \cup \Sigma, \\ \operatorname{Tr}(F : D(\bar{\rho})) & \textit{if } p = \ell \notin S_{\bar{\rho}}, \\ \bar{\rho}_{I_p}(\varphi_p) & \textit{if } p \in S_{\bar{\rho}}, \\ 0 & \textit{if } p \neq \ell, \in \Sigma. \end{cases} \tag{10.1}$$

PROOF. Since $T(N_\Sigma)_\mathcal{O}$ is generated by T_p (p: prime), the uniqueness is clear. We show the existence.

First, we show it when $\Sigma = \varnothing$. By Corollary 3.56, $\bar{\rho}$ is modular of level $N_{\bar{\rho}} = N_\varnothing$. Thus, by Lemma 9.22 and Corollary 9.23(1), there exists a ring homomorphism $\overline{\varphi} : T_0(N_\varnothing)_\mathbf{Z} \to \mathbf{F}'$ to a finite extension $\mathbf{F}'$ of $\mathbf{F}$ that satisfies

$$\det(1 - \bar{\rho}(\varphi_p)t) = 1 - \overline{\varphi}(T_p)t + pt^2$$

for all prime numbers $p \nmid N_\varnothing \ell$. If $\ell \notin S_{\bar{\rho}}$, we have $\ell \nmid N_\varnothing$, and by Corollary 9.23(2), $\bar{\rho}$ is good at ℓ and $\det(1 - Ft : D(\bar{\rho})) = 1 - \overline{\varphi}(T_\ell)t + \ell t^2$. If $p \in S_{\bar{\rho}}$, then $\bar{\rho}$ is ordinary at p and bad at p. Thus, by Corollary 9.48(1), we have $\bar{\rho}_{I_p}(\varphi_p) = \overline{\varphi}(T_p)$. Hence, $\overline{\varphi} : T(N_\varnothing)_\mathcal{O} \to \mathbf{F}'$ satisfies the condition (10.1), and its image is contained in $\mathbf{F}$. This proves the case $\Sigma = \varnothing$.

Next, we show the general case. For $p \in \Sigma$, define a polynomial $P_p(U) \in T(N_\varnothing)_\mathcal{O}[U]$ as in (9.34) by

$$P_p(U) = \begin{cases} U(U^2 - T_pU + p) & \text{if } p \neq \ell, \\ U^2 - T_\ell U + \ell & \text{if } p = \ell. \end{cases} \tag{10.2}$$

Define a ring homomorphism

$$T(N_\Sigma)_\mathcal{O} \to T(N_\varnothing)_\mathcal{O}[U_p, p \in \Sigma]/(P_p(U_p), p \in \Sigma)$$

using Corollary 9.37 repeatedly, and sending T_p to T_p if $p \notin \Sigma$, and T_p to U_p if $p \in \Sigma$. We denote by $\overline{P}_p(U) \in \mathbf{F}[U]$ the image of $P_p(U)$ by the ring homomorphism $\overline{\varphi}_\varnothing : T(N_\varnothing)_\mathcal{O} \to \mathbf{F}$. If $\ell \in \Sigma$, we have $\bar{P}_\ell(U) = U(U - \overline{\varphi}_\varnothing(T_\ell))$.

Define a ring homomorphism $\mathbf{F}[U_p, p \in \Sigma]/(\bar{P}_p(U_p), p \in \Sigma) \to \mathbf{F}$ by sending the image of U_p to 0 if $p \neq \ell$, and to $\overline{\varphi}_\varnothing(T_\ell)$ if $p = \ell \in \Sigma$. It is clear from the definition that the composition

$$\begin{aligned} \overline{\varphi}_\Sigma : T(N_\Sigma)_\mathcal{O} &\longrightarrow T(N_\varnothing)_\mathcal{O}[U_p, p \in \Sigma]/(P_p(U_p), p \in \Sigma) \\ &\xrightarrow{\overline{\varphi}_\varnothing} \mathbf{F}[U_p, p \in \Sigma]/(\bar{P}_p(U_p), p \in \Sigma) \longrightarrow \mathbf{F} \end{aligned}$$

satisfies condition (10.1). □

DEFINITION 10.2. Let $\mathfrak{m}_\Sigma$ be the kernel of the surjective ring homomorphism $T(N_\Sigma)_\mathcal{O} \to \mathbf{F}$. The completion $T(N_\Sigma)_{\mathcal{O},\mathfrak{m}_\Sigma}$ of $T(N_\Sigma)_\mathcal{O}$ at the maximal ideal $\mathfrak{m}_\Sigma$ is called the *full Hecke algebra*, and we denote it by $T^\flat_\Sigma$.

Since $T(N_\Sigma)_\mathcal{O}$ is finitely generated as an $\mathcal{O}$-module, it is a complete semilocal ring and decomposes into the product of local rings. Thus, the completion $T(N_\Sigma)_{\mathcal{O},\mathfrak{m}_\Sigma}$ equals the localization of $T(N_\Sigma)_\mathcal{O}$ at the maximal ideal $\mathfrak{m}_\Sigma$.

LEMMA 10.3. *The full Hecke algebra $T^\flat_\Sigma$ is a finitely generated free $\mathcal{O}$-module.*

PROOF. The $\mathcal{O}$-module $T(N_\Sigma)_\mathcal{O}$ is finitely generated and free since the $\mathbf{Z}$-module $T(N_\Sigma)_\mathbf{Z}$ is finitely generated and free. Since the $\mathcal{O}$-module $T^\flat_\Sigma$ is a direct summand of $T(N_\Sigma)_\mathcal{O}$, it is also finitely generated and free. □

We now study the relation between the full Hecke algebra $T^\flat_\Sigma$ and the reduced Hecke algebra T_Σ defined in Definition 5.16. Let $T(N_\Sigma)'_\mathcal{O}$ be the subring of $T(N_\Sigma)_\mathcal{O}$ generated by T_p, $p \nmid N_\Sigma \ell$,

$$T(N_\Sigma)'_\mathcal{O} = \mathcal{O}[T_p, p \nmid N_\Sigma \ell] \subset T(N_\Sigma)_\mathcal{O},$$

and define a maximal ideal $\mathfrak{m}'_\Sigma$ of $T(N_\Sigma)'_\mathcal{O}$ as the inverse image of $\mathfrak{m}_\Sigma$ by the inclusion $T(N_\Sigma)'_\mathcal{O} \to T(N_\Sigma)_\mathcal{O}$. By Corollary 2.60, $T'(N_\Sigma)_K = T'(N_\Sigma)_\mathcal{O} \otimes_\mathcal{O} K$ coincides with the reduced Hecke algebra $T'(N_\Sigma)_K$ in Definition 2.57.

PROPOSITION 10.4. (1) *As a subset of the set $\Phi(N_\Sigma)_K$ of primitive forms over K defined as* $\operatorname{Spec} T(N_\Sigma)'_K$*, the set $\Phi(N_\Sigma)_{K,\bar\rho}$ is equal to* $\operatorname{Spec} T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} \otimes_\mathcal{O} K$. *The reduced Hecke algebra T_Σ coincides with the localization $T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma}$ of $T(N_\Sigma)'_\mathcal{O}$ at $\mathfrak{m}'_\Sigma$:*

$$T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} = T_\Sigma. \tag{10.3}$$

(2) *The morphism of $\mathcal{O}$-algebras induced by the inclusion $T(N_\Sigma)'_\mathcal{O} \to T(N_\Sigma)_\mathcal{O}$*

$$i_\Sigma : T_\Sigma = T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} \longrightarrow T^\flat_\Sigma = T(N_\Sigma)_{\mathcal{O},\mathfrak{m}_\Sigma} \tag{10.4}$$

is injective and induces an isomorphism $T_{\Sigma,K} \to T^\flat_{\Sigma,K}$.

In Theorem 10.46, we will show $i_\Sigma : T_\Sigma \to T^\flat_\Sigma$ is an isomorphism.

PROOF. (1) We show $\Phi(N_\Sigma)_{K,\bar{\rho}} = \operatorname{Spec} T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} \otimes_{\mathcal{O}} K$. Let $f \in \Phi(N_\Sigma)_K$ be a primitive form. The image of the homomorphism $T(N_\Sigma)'_{\mathcal{O}} \to T(N_\Sigma)'_K \to K_f$ is in the ring of integers $\mathcal{O}_f$, and the inverse image $\mathfrak{m}_f$ of the maximal ideal $\mathcal{O}_f$ is the unique maximal ideal of $T(N_\Sigma)'_{\mathcal{O}}$ containing $\operatorname{Ker}(T(N_\Sigma)'_{\mathcal{O}} \to K_f)$. Thus, we have

$$\operatorname{Spec} T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} \otimes_{\mathcal{O}} K = \{f \in \Phi(N_\Sigma)_K \mid \mathfrak{m}_f = \mathfrak{m}'_\Sigma\}.$$

On the other hand, by Definition 5.13, we have

$$\Phi(N_\Sigma)_{K,\bar{\rho}} = \left\{ f \in \Phi(N_\Sigma)_K \;\middle|\; \begin{array}{l} T_p \;\equiv\; \operatorname{Tr}\bar{\rho}(\varphi_p) \bmod \mathfrak{m}_f \\ \text{for all prime } p \nmid N_\Sigma \ell \end{array} \right\}.$$

The restriction $T(N_\Sigma)'_{\mathcal{O}} \to \mathbf{F}$ of $\overline{\varphi}_\Sigma$ is determined by $\overline{\varphi}_\Sigma(T_p) = \operatorname{Tr}\bar{\rho}(\varphi_p)$ for $p \nmid N_\Sigma \ell$, and $\mathfrak{m}'_\Sigma$ is its kernel. Thus, the right-hand side of the above two formulas are equal.

Since $T(N_\Sigma)'_K$ is reduced by Proposition 2.58, its subring $T(N_\Sigma)'_{\mathcal{O}}$ is reduced and so is its localization $T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma}$. Thus, $T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} \to T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} \otimes_{\mathcal{O}} K = \prod_{f \in \Phi(N_\Sigma)_{K,\bar{\rho}}} K_f$ is injective. $T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma}$ is a subring of $T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma} \otimes_{\mathcal{O}} K = \prod_{f \in \Phi(N_\Sigma)_{K,\bar{\rho}}} K_f$ generated by $T_p (p \nmid N_\Sigma \ell)$ over $\mathcal{O}$. Thus, by Definition 5.16, $T_\Sigma = T(N_\Sigma)'_{\mathcal{O},\mathfrak{m}'_\Sigma}$.

(2) Since T_Σ is a finitely generated free $\mathcal{O}$-module, it suffices to show that $i_\Sigma : T_\Sigma \to T^\flat_\Sigma$ induces an isomorphism $T_{\Sigma,K} \to T^\flat_{\Sigma,K}$. Since $T_{\Sigma,K} = \prod_{f \in \Phi(N_\Sigma)_{K,\bar{\rho}}} K_f$, it suffices to show that $K_f \to T^\flat_{\Sigma,K} \otimes_{T_{\Sigma,K}} K_f$ is an isomorphism for each primitive form $f \in \Phi(N_\Sigma)_{K,\bar{\rho}}$.

Let f be a primitive form belonging to $\Phi(N_\Sigma)_{K,\bar{\rho}}$, and $N_f | N_\Sigma$ the level of f. By definition, $N_\varnothing$ is the product of p at which $\bar{\rho}$ is bad. The mod ℓ reduction of ρ_f is isomorphic to $\bar{\rho}$, and ρ_f is bad at the prime p where $\bar{\rho}$ is bad. By Theorem 3.52(1), a prime p at which ρ_f is bad divides N_f, and we have $N_\varnothing \mid N_f$. Thus, if $p \mid N_\Sigma / N_f$, then $p \in \Sigma$. For a prime $p \mid N_\Sigma / N_f$, define a polynomial $P_{f,p}(U) \in \mathcal{O}_f[U]$ as in (9.37) by

$$P_{f,p}(U) = \begin{cases} U(U^2 - a_p(f)U + p) & \text{if } \operatorname{ord}_p N_\Sigma/N_f = 2, \\ U(U - a_p(f)) & \operatorname{ord}_p N_\Sigma/N_f = 1 \text{ and } p \mid N_f, \\ U^2 - a_p(f)U + p & \operatorname{ord}_p N_\Sigma/N_f = 1 \text{ and } p \nmid N_f. \end{cases}$$

By Corollary 9.41, we have

$$T(N_\Sigma)_{\mathbf{Q}} \otimes_{T'(N_\Sigma)_{\mathbf{Q}}} K_f = K_f[U_p, p | N_\Sigma/N_f]/(P_{f,p}(U_p), p | N_\Sigma/N_f).$$

Thus, if we let $A_f = \mathcal{O}_f[U_p, p | N_\Sigma/N_f]/(P_{f,p}(U_p), p | N_\Sigma/N_f)$, we obtain a morphism of $\mathcal{O}$-algebras $T(N_\Sigma)_{\mathcal{O}} \to A_f$ by sending the image of T_p to $a_p(f)$ if $p \nmid N_\Sigma/N_f$, and U_p if $p|N_\Sigma/N_f$. Moreover, we have

$$\begin{aligned} &T^\flat_{\Sigma,K} \otimes_{T_{\Sigma,K}} K_f \\ &\qquad = T^\flat_{\Sigma,K} \otimes_{T(N_\Sigma)_K} K_f[U_p, p|N_\Sigma/N_f]/(P_{f,p}(U_p), p|N_\Sigma/N_f) \\ &\qquad = (T^\flat_\Sigma \otimes_{T(N_\Sigma)_\mathcal{O}} A_f) \otimes_\mathcal{O} K. \end{aligned}$$

Thus, it suffices to show that $\mathcal{O}_f \to T^\flat_\Sigma \otimes_{T(N_\Sigma)_\mathcal{O}} A_f$ is an isomorphism.

Since A_f is finitely generated as an $\mathcal{O}$-module, it is a complete semilocal ring, and it decomposes to the product of local rings. $T^\flat_\Sigma$ is by definition the localization of $T(N_\Sigma)_\mathcal{O}$ at $\mathfrak{m}_\Sigma$. Thus, it suffices to show that there is a unique maximal ideal $\mathfrak{m}$ of A_f lying above $\mathfrak{m}_\Sigma$, and the local ring $A_{f,\mathfrak{m}}$ is isomorphic to $\mathcal{O}_f$. Let $\mathbf{F}_f$ be the residue field of $\mathcal{O}_f$. By the definition (10.1) of $\mathfrak{m}_\Sigma$, a maximal ideal $\mathfrak{m}$ lies above $\mathfrak{m}_\Sigma$ if and only if for each prime number $p \in \Sigma$

$$a_p(f) \equiv \begin{cases} \mathrm{Tr}(F : D(\bar\rho)) \mod \mathfrak{m} & \text{if } p = \ell \notin S_{\bar\rho}, \\ 0 \mod \mathfrak{m} & \text{if } p \neq \ell, \in \Sigma, \end{cases} \tag{10.5}$$

if $p \nmid N_\Sigma/N_f$, and

$$U_p \equiv \begin{cases} \mathrm{Tr}(F : D(\bar\rho)) \mod \mathfrak{m} & \text{if } p = \ell \notin S_{\bar\rho}, \\ 0 \mod \mathfrak{m} & \text{if } p \neq \ell, \in \Sigma, \end{cases} \tag{10.6}$$

if $p|N_\Sigma/N_f$. Thus, if $\mathfrak{m}$ exists, it is unique.

If $p = \ell \in \Sigma$ and $\ell \nmid N_\Sigma/N_f$, then $\ell \notin S_{\bar\rho}$ and $\ell|N_f$. In this case, by Corollary 9.48(2), we have $a_p(f) \equiv \mathrm{Tr}(F : D(\bar\rho))$. If $p \neq \ell$, $p \in \Sigma$ and $p \nmid N_\Sigma/N_f$, then $\mathrm{ord}_p N_f = 2$. Thus, by Corollary 9.39(2), we have $a_p(f) = 0$. If $p = \ell|N_\Sigma/N_f$, then $p \nmid N_f$. Thus, by Corollary 9.23(2), we have $P_{f,\ell}(U) \equiv U(U - \mathrm{Tr}(F : D(\bar\rho)))$. In this case, $\bar\rho$ is ordinary at ℓ, and again by Corollary 9.23(2), we have $\mathrm{Tr}(F : D(\bar\rho)) \neq 0$. Thus, in this case, the multiplicity of the root $\mathrm{Tr}(F : D(\bar\rho))$ of $P_{f,\ell}(U) \equiv U(U - \mathrm{Tr}(F : D(\bar\rho))) \in \mathbf{F}_f[U]$ is 1. Suppose $p|N_\Sigma/N_f$ and $p \neq \ell$. If $p|N_f$, then $a_p(f) = \pm 1$ by Proposition 9.47 and the multiplicity of the root 0 of $P_{p,f}(U) \equiv U(U - \overline{a_p(f)}) \in \mathbf{F}_f[U]$ is one. If $p \nmid N_f$, the multiplicity of the root 0 of $P_{p,f}(U) \equiv U(U^2 - \overline{a_p(f)}U + p) \in \mathbf{F}_f[U]$ is 1.

Thus, the only maximal ideal $\bar{\mathfrak{m}}$ of

$$A_{f,\mathbf{F}_f} = \mathbf{F}_f[U_p, p|N_\Sigma/N_f]/(P_{f,p}(U_p), p|N_\Sigma/N_f),$$

whose pullback equals $\mathfrak{m}_\Sigma$, is $\overline{\mathfrak{m}} = \big(U_p\ (p \neq \ell, p|N_\Sigma/N_f),\ U_\ell - \mathrm{Tr}(F : D(\bar\rho))\ (\text{if } \ell|N_\Sigma/N_f)\big)$. Moreover, the local ring $A_{f,\mathbf{F}_f,\overline{\mathfrak{m}}}$ is isomorphic to $\mathbf{F}_f$. Hence, there exists a unique maximal ideal $\mathfrak{m}$ of A_f lying above $\mathfrak{m}_\Sigma$, and the local ring $A_{f,\mathfrak{m}}$ is isomorphic to $\mathcal{O}_f$. ☐

COROLLARY 10.5. *The full Hecke algebra $T_\Sigma^\flat$ is also reduced.*

PROOF. By Lemma 10.3 and Proposition 10.4(2), we have $T_\Sigma^\flat \subset T_{\Sigma,K}^\flat = T_{\Sigma,K} = \prod_{f\in\Phi(N_\Sigma)_{K,\bar\rho}} K_f$. ☐

Let Σ' be a finite set of prime numbers that does not intersect with $S_{\bar\rho}$. If $\ell \notin \Sigma'$ and $\bar\rho$ is good and ordinary at $p=\ell$, T_ℓ is an invertible element of $T_\varnothing^\flat$ by Corollary 9.48(2). By Hensel's lemma, there exists a unique root of $U^2 - T_\ell U + \ell$ that is an invertible element of $T_{\Sigma'}^\flat$. In what follows, we denote it by $T_\ell^\sharp$.

PROPOSITION 10.6. *Let $\Sigma = \Sigma' \amalg \{p\}$. There exists a unique morphism of $\mathcal{O}$-algebras $t_{\Sigma',\Sigma}^\flat : T_\Sigma^\flat \to T_{\Sigma'}^\flat$ satisfying the condition*

$$t_{\Sigma',\Sigma}^\flat(T_q) = \begin{cases} T_q & \text{if } q \neq p, \\ 0 & \text{if } q = p \neq \ell, \\ T_\ell^\sharp & \text{if } q = p = \ell. \end{cases} \tag{10.7}$$

PROOF. The uniqueness is clear. Let $P_p(U) \in T(N_\varnothing)[U]$ be the polynomial we defined by (10.2) in the proof of Proposition 10.1. Let $A_{\Sigma'} = T(N_{\Sigma'})_{\mathcal{O}}[U]/(P_p(U))$. Define a ring homomorphism $T(N_\Sigma)_{\mathcal{O}} \to A_{\Sigma'}$ by sending T_p to U as in Corollary 9.37. Define a ring homomorphism $T_{\Sigma'}^\flat \otimes_{T(N_{\Sigma'})_{\mathcal{O}}} A_{\Sigma'} \to T_{\Sigma'}^\flat$ by letting the image of U equal to 0 if $p \neq \ell$, and $T_\ell^\sharp$ if $p = \ell$. The inverse image of the maximal ideal of $T_{\Sigma'}^\flat$ by the composition

$$T(N_\Sigma)_{\mathcal{O}} \longrightarrow A_{\Sigma'} \longrightarrow T_{\Sigma'}^\flat \otimes_{T(N_{\Sigma'})_{\mathcal{O}}} A_{\Sigma'} \longrightarrow T_{\Sigma'}^\flat \tag{10.8}$$

is $\mathfrak{m}_\Sigma$, and a ring homomorphism $T_\Sigma^\flat \to T_{\Sigma'}^\flat$ is induced. It is clear that this homomorphism satisfies the condition. ☐

The restriction of $t_{\Sigma',\Sigma}^\flat : T_\Sigma^\flat \to T_{\Sigma'}^\flat$ to T_Σ is nothing but $t_{\Sigma',\Sigma} : T_\Sigma \to T_{\Sigma'}$ defined in §5.5 in Chapter 5.

10.2. Hecke modules

In this section we define the Hecke module M_Σ as the completion of the singular cohomology of a modular curve, and we construct *RTM*-triples.

DEFINITION 10.7. We regard the $T^{\flat}_{\Sigma}$-module

$$M_{\Sigma} = H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})_{\mathcal{O}} \otimes_{T(N_{\Sigma})_{\mathcal{O}}} T^{\flat}_{\Sigma}$$

as a T_{Σ}-module through the ring homomorphism $i_{\Sigma} : T_{\Sigma} \to T^{\flat}_{\Sigma}$, and we call it *Hecke module.*

In this chapter we may omit the superscript ${}^{\mathrm{an}}$ to indicate a complex manifold. For example, we sometimes write $H_1(X_0(N), \mathbf{Z})_{\mathcal{O}}$ instead of $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})_{\mathcal{O}}$.

PROPOSITION 10.8. *Let $f \in \Phi(N_{\varnothing})_{K,\bar{\rho}}(K)$ be a primitive form with K coefficients, and let $\pi_{\Sigma} : T_{\Sigma} \to \mathcal{O}$ be the ring homomorphism defined by f. Then, the RTM-triple*

$$\mathcal{R}_{\Sigma} = (R_{\Sigma}, T_{\Sigma}, M_{\Sigma}, f_{\Sigma} : R_{\Sigma} \to T_{\Sigma}, \pi_{\Sigma} : T_{\Sigma} \to \mathcal{O})$$

is an RTM-triple of rank 2.

PROOF. We verify the conditions of Definition 5.26. For the first three objects, R_{Σ} is a profinitely generated complete local $\mathcal{O}$-algebra, T_{Σ} is a local $\mathcal{O}$-algebra, and M_{Σ} is a T_{Σ}-module. As we remarked after Definition 5.16, T_{Σ} is finitely generated as an $\mathcal{O}$-module. Since $H_1(X_0(N), \mathbf{Z})$ is a finitely generated free $\mathbf{Z}$-module, M_{Σ} is a finitely generated free $\mathcal{O}$-module. Since $T_{\Sigma,K} = T^{\flat}_{\Sigma,K}$, $M_{\Sigma,K}$ is a free $T_{\Sigma,K}$-module of rank 2 by Proposition 9.6. If we let $\mathfrak{p}_{T_{\Sigma}} = \mathrm{Ker}\ \pi_{\Sigma}$, we have $\mathfrak{p}_{T_{\Sigma}}/\mathfrak{p}^2_{T_{\Sigma}} \otimes_{\mathcal{O}} K = 0$ since T_{Σ} is reduced. Thus, the finitely generated $\mathcal{O}$-module $\mathfrak{p}_{T_{\Sigma}}/\mathfrak{p}^2_{T_{\Sigma}}$ has finite length. ☐

We will show in Theorem 10.46 that M_{Σ} is a free T_{Σ}-module of rank 2.

Let $\Sigma = \Sigma' \amalg \{p\}$, and we define morphisms of Hecke modules $m_{\Sigma',\Sigma} : M_{\Sigma} \to M_{\Sigma'}$ and $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_{\Sigma}$. First we define $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_{\Sigma}$ as follows. Let $s^*_i : H_1(X_0(N_{\Sigma'}), \mathbf{Z})_{\mathcal{O}} \to H_1(X_0(N_{\Sigma}), \mathbf{Z})_{\mathcal{O}}$ be the pullback of the morphism of modular curves s_{p^i} as in §§9.4–9.5.

LEMMA 10.9. *Let $\Sigma = \Sigma' \amalg \{p\}$. Define an $\mathcal{O}$-linear mapping $m^* : M_{\Sigma'} \to H_1(X_0(N_{\Sigma}), \mathbf{Z})_{\mathcal{O}}$ by*

$$\begin{cases} s^*_0|_{M_{\Sigma'}} - s^*_1|_{M_{\Sigma'}} \circ T_p \cdot + p \cdot s^*_2|_{M_{\Sigma'}} & \textit{if } p \neq \ell, \\ s^*_0|_{M_{\Sigma'}} - s^*_1|_{M_{\Sigma'}} \circ T^{\sharp}_{\ell} \cdot & \textit{if } p = \ell. \end{cases} \tag{10.9}$$

The $\mathcal{O}$-linear mapping $m^* : M_{\Sigma'} \to H_1(X_0(N_{\Sigma}), \mathbf{Z})_{\mathcal{O}}$ induces an $\mathcal{O}$-linear mapping $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_{\Sigma}$ compatible with the ring homomorphism $t^{\flat}_{\Sigma,\Sigma'} : T^{\flat}_{\Sigma} \to T^{\flat}_{\Sigma'}$.

PROOF. As in the proof of Proposition 10.6, define a polynomial $P_p(U) \in T(N_\varnothing)[U]$ by (10.2), and let $A_{\Sigma'} = T(N_{\Sigma'})_\mathcal{O}[U]/(P_p(U))$.

We first show the case $p \neq \ell$. As in (9.30), define a matrix $U_p \in M_3(T(N_{\Sigma'})_\mathcal{O})$ by $U_p = \begin{pmatrix} 0 & 0 & 0 \\ p & 0 & -1 \\ 0 & p & T_p \end{pmatrix}$. Considering the action of U as the multiplication-by-U_p, we regard $H_1(X_0(N_{\Sigma'}), \mathbf{Z})^3_\mathcal{O}$ as an $A_{\Sigma'}$-module. By Proposition 9.36, the morphism $(s_0^*, s_1^*, s_2^*) : H_1(X_0(N_{\Sigma'}), \mathbf{Z})^3_\mathcal{O} \to H_1(X_0(N_\Sigma), \mathbf{Z})_\mathcal{O}$ is compatible with the ring homomorphism $T(N_\Sigma)_\mathcal{O} \to A_{\Sigma'}$. Since $U_p \begin{pmatrix} 1 \\ -T_p \\ p \end{pmatrix} = 0$, the $\mathcal{O}$-linear mapping $(1, -T_p, p) : M_{\Sigma'} \to H_1(X_0(N_{\Sigma'}), \mathbf{Z})^3_\mathcal{O}$ is compatible with the ring homomorphism $A_{\Sigma'} \dashrightarrow T^\flat_{\Sigma'} \otimes_{T(N_{\Sigma'})_\mathcal{O}} A_{\Sigma'} \to T^\flat_{\Sigma'}$ defined by letting the image of U_p be equal to 0. The linear mapping $m^* : M_{\Sigma'} \dashrightarrow H_1(X_0(N_\Sigma), \mathbf{Z})_\mathcal{O}$ is the composition of these linear mappings, and thus it is compatible with the ring homomorphism $T(N_\Sigma)_\mathcal{O} \to A_{\Sigma'} \to T^\flat_{\Sigma'}$. $t^\flat_{\Sigma',\Sigma} : T^\flat_\Sigma \to T^\flat_{\Sigma'}$ is induced by this composition of ring homomorphisms. This shows the case $p \neq \ell$.

In the case of $p = \ell$, define the action of U on $H_1(X_0(N_{\Sigma'}), \mathbf{Z})^2_\mathcal{O}$ by the multiplication of the matrix $U_\ell = \left(\begin{smallmatrix} 0 & -1 \\ \ell & T_\ell \end{smallmatrix}\right) \in M_2(T_0(N_{\Sigma'})_\mathcal{O})$. Since $U_\ell \left(\begin{smallmatrix} 1 \\ -T_\ell^\sharp \end{smallmatrix}\right) = T_\ell^\sharp \left(\begin{smallmatrix} 1 \\ -T_\ell^\sharp \end{smallmatrix}\right)$, the rest of the proof is similar to the case $p \neq \ell$. □

COROLLARY 10.10. *Let* $\Sigma = \Sigma' \amalg \{p\}$. *We denote by* $\bar{s}_{i*}$ *the composition of natural surjection* $H_1(X_0(N_{\Sigma'}), \mathbf{Z})_\mathcal{O} \to M_{\Sigma'}$ *and* $s_{i*} : H_1(X_0(N_\Sigma), \mathbf{Z})_\mathcal{O} \to H_1(X_0(N_{\Sigma'}), \mathbf{Z})_\mathcal{O}$, *and define a morphism of* $\mathcal{O}$-*modules* $m_* : H_1(X_0(N_\Sigma), \mathbf{Z})_\mathcal{O} \to M_{\Sigma'}$ *by*

$$m_* = \begin{cases} p \cdot \bar{s}_{0*} - T_p \cdot \bar{s}_{1*} + \bar{s}_{2*} & \text{if } p \neq \ell, \\ -T_\ell^\sharp \cdot \bar{s}_{0*} + \bar{s}_{1*} & \text{if } p = \ell. \end{cases} \tag{10.10}$$

Then, the morphism $m_* : H_1(X_0(N_\Sigma), \mathbf{Z})_\mathcal{O} \to M_{\Sigma'}$ *induces a morphism of* $\mathcal{O}$-*modules* $m_{\Sigma',\Sigma} : M_\Sigma \to M_{\Sigma'}$ *that is compatible with the ring homomorphism* $t^\flat_{\Sigma',\Sigma} : T^\flat_\Sigma \to T^\flat_{\Sigma'}$.

PROOF. The isomorphism of $T(N_\Sigma)_\mathbf{Z}$-modules

$$H_1(X_0(N_\Sigma), \mathbf{Z}) \to \mathrm{Hom}(H_1(X_0(N_\Sigma), \mathbf{Z}), \mathbf{Z}); x \mapsto (y \mapsto (x, wy)) \tag{9.4}$$

induces an isomorphism of $T^\flat_\Sigma$-modules $M_\Sigma \to \mathrm{Hom}_\mathcal{O}(M_\Sigma, \mathcal{O})$, and similarly, an isomorphism of $T^\flat_{\Sigma'}$-modules $M_{\Sigma'} \to \mathrm{Hom}_\mathcal{O}(M_{\Sigma'}, \mathcal{O})$. Let $m^{*\vee}_{\Sigma',\Sigma} : \mathrm{Hom}_\mathcal{O}(M_\Sigma, \mathcal{O}) \to \mathrm{Hom}_\mathcal{O}(M_{\Sigma'}, \mathcal{O})$ be the dual of $m^*_{\Sigma',\Sigma}$:

$M_{\Sigma'} \dashrightarrow M_\Sigma$. It suffices to show that the mapping (10.10) induces the composition

$$(10.11) \quad M_\Sigma \longrightarrow \operatorname{Hom}_{\mathcal{O}}(M_\Sigma, \mathcal{O}) \xrightarrow{m^{*\vee}_{\Sigma',\Sigma}} \operatorname{Hom}_{\mathcal{O}}(M_{\Sigma'}, \mathcal{O}) \longrightarrow M_{\Sigma'}.$$

We show the case $p \neq \ell$. By the definition of $m^*_{\Sigma',\Sigma}$, the composition (10.11) is induced by $w \circ (\bar{s}_{0*} - T^*_p \cdot \bar{s}_{1*} + p \cdot \bar{s}_{2*}) \circ w$. Since $p \nmid N_{\Sigma'}$, we have $T^*_p = T_p$ by Lemma 9.5, and $w \circ T_p = T_p \circ w$. Moreover, since $w \circ s_i = s_{2-i} \circ w : X_0(N_\Sigma) \to X_0(N_{\Sigma'})$, (10.11) is induced by $\bar{s}_{2*} - T_p \cdot \bar{s}_{1*} + p \cdot \bar{s}_{0*}$. This shows the case $p \neq \ell$.

In the case of $p = \ell$, we prove it similarly using the fact that $w \circ (\bar{s}_{0*} - T^\sharp_\ell \cdot \bar{s}_{1*}) \circ w = \bar{s}_{1*} - T^\sharp_\ell \cdot \bar{s}_{0*}$ □

PROPOSITION 10.11. *If $\Sigma = \Sigma' \amalg \{p\}$, then $m_{\Sigma',\Sigma} : M_\Sigma \dashrightarrow M_{\Sigma'}$ is surjective.*

The proof will be given in the next section. Proposition 5.30 in Chapter 5 follows from Proposition 10.11 by the induction on the number of elements in $\Sigma - \Sigma'$.

COROLLARY 10.12. *If $\Sigma = \Sigma' \amalg \{p\}$, then $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_\Sigma$ is injective, and its image is a direct summand as an $\mathcal{O}$-module.*

PROOF. By the proof of Corollary 10.10, $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_\Sigma$ is the dual of $m_{\Sigma',\Sigma} : M_\Sigma \to M_{\Sigma'}$. Thus, the assertion follows immediately from Proposition 10.11. □

PROPOSITION 10.13. *Let $f \in \Phi(N_\varnothing)_{K,\bar\rho}(K)$ be a primitive form with K-coefficients, and let $\pi_\Sigma : T_\Sigma \to \mathcal{O}$ be a ring homomorphism defined by f. If $\Sigma = \Sigma' \amalg \{p\}$, then the quadruple*

$$\begin{aligned}\mathcal{F}_{\Sigma',\Sigma} = (&r_{\Sigma',\Sigma} : R_\Sigma \to R_{\Sigma'}, t_{\Sigma',\Sigma} : T_\Sigma \to T_{\Sigma'},\\ &m_{\Sigma',\Sigma} : M_\Sigma \to M_{\Sigma'}, m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_\Sigma)\end{aligned}$$

is a surjection of RTM-triples $\mathcal{R}_\Sigma \to \mathcal{R}_{\Sigma'}$.

PROOF. $r_{\Sigma',\Sigma} : R_\Sigma \to R_{\Sigma'}$ and $t_{\Sigma',\Sigma} : T_\Sigma \to T_{\Sigma'}$ are surjective local morphisms of local $\mathcal{O}$-algebras, and the diagram

$$\begin{tikzcd}
R_\Sigma \arrow[r, "f_\Sigma"] \arrow[d, "r_{\Sigma',\Sigma}"'] & T_\Sigma \arrow[r, "\pi_\Sigma"] \arrow[d, "t_{\Sigma',\Sigma}"] & \mathcal{O} \arrow[d, equal] \\
R_{\Sigma'} \arrow[r, "f_{\Sigma'}"'] & T_{\Sigma'} \arrow[r, "\pi_{\Sigma'}"'] & \mathcal{O}
\end{tikzcd}$$

is commutative. $m_{\Sigma',\Sigma} : M_\Sigma \to M_{\Sigma'}$ and $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_\Sigma$ are $\mathcal{O}$-linear mappings compatible with $t_{\Sigma',\Sigma}$. By Proposition 10.11, $m_{\Sigma',\Sigma} : M_\Sigma \to M_{\Sigma'}$ is surjective. By Corollary 10.12, $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_\Sigma$ is injective, and its image is a direct summand as an $\mathcal{O}$-module. ☐

PROPOSITION 10.14. *Let* $\Sigma = \Sigma' \amalg \{p\}$. *Define an element* Δ_p *in* $T^\flat_{\Sigma'}$ *by*

$$\Delta_p = \begin{cases} (p-1)((p+1)^2 - T_p^2) & \text{if } p \neq \ell, \\ (T_p^{\sharp 2} - 1)(2T_p^\sharp - T_p) & \text{if } p = \ell. \end{cases}$$

Suppose also $\Delta_p \in T_{\Sigma'}$ *when* $p = \ell$. *Then* Δ_p *is the multiplier of the surjection* $\mathcal{F}_{\Sigma',\Sigma}$ *of RTM-triples.*

Proposition 5.33 in Chapter 5 follows from Proposition 10.14.

PROOF. It suffices to show that the composition $m_{\Sigma',\Sigma} \circ m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_{\Sigma'}$ is the multiplication-by-Δ_p mapping. We show the case $p \neq \ell$. By the definition of $m_{\Sigma',\Sigma}$ and $m^*_{\Sigma',\Sigma}$, the composition $m_{\Sigma',\Sigma} \circ m^*_{\Sigma',\Sigma}$ is induced by multiplication by

$$\begin{pmatrix} p & -T_p & 1 \end{pmatrix} \begin{pmatrix} s_{0*} \circ s_0^* & s_{0*} \circ s_1^* & s_{0*} \circ s_2^* \\ s_{1*} \circ s_0^* & s_{1*} \circ s_1^* & s_{1*} \circ s_2^* \\ s_{2*} \circ s_0^* & s_{2*} \circ s_1^* & s_{2*} \circ s_2^* \end{pmatrix} \begin{pmatrix} 1 \\ -T_p \\ p \end{pmatrix}.$$

We show

$$s_{i*} \circ s_j^* = \begin{cases} p(p+1) & \text{if } i = j, \\ pT_p & \text{if } i = j \pm 1, \\ T_p^2 - (p+1) & \text{if } i = j \pm 2. \end{cases}$$

If $j = j$, then $s_{i*} \circ s_i^* = \deg s_i = p(p+1)$. Let $t_0, t_1 : X_0(N_\Sigma) \to X_0(N_{\Sigma'}p)$ and $r_0, r_1 : X_0(N_{\Sigma'}p) \to X_0(N_{\Sigma'})$ be morphisms s_1 and s_p in (8.65). By Lemma 9.35(1), we have $s_{0*} \circ s_1^* = r_{0*} \circ t_{0*} \circ t_0^* \circ r_1^* = \deg t_0 \cdot r_{0*} \circ r_1^* = pT_p$. By Lemma 9.5(2), we have $s_{1*} \circ s_0^* = pT_p^* = pT_p$. Similar statements hold for $s_{2*} \circ s_1^*$ and $s_{1*} \circ s_2^*$. By the proof of Proposition 9.38(1), we have $t_{0*} \circ t_1^* + w = r_1^* \circ r_{0*}$. Thus, we have

$$\begin{aligned} s_{0*} \circ s_2^* &= r_{0*} \circ r_1^* \circ r_{0*} \circ r_1^* - r_{0*} \circ w_* \circ r_1^* \\ &= T_p^2 - \deg r_{0*} = T_p^2 - (p+1). \end{aligned}$$

The same is true for $s_{2*} \circ s_0^*$. Thus, in the case $p \neq \ell$, the assertion follows from the equality

$$\begin{aligned} &\begin{pmatrix} p & -T_p & 1 \end{pmatrix} \begin{pmatrix} p(p+1) & pT_p & T_p^2-(p+1) \\ pT_p & p(p+1) & pT_p \\ T_p^2-(p+1) & pT_p & p(p+1) \end{pmatrix} \begin{pmatrix} 1 \\ -T_p \\ p \end{pmatrix} \\ &= \begin{pmatrix} p & -T_p & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ (p^2-1)(p+1)-(p-1)T_p^2 \end{pmatrix} \\ &= (p-1)\big((p+1)^2 - T_p^2\big). \end{aligned}$$

Similarly, in the case $p = \ell$, since we have $p = T_p^\sharp T_p - T_p^{\sharp 2}$, the assertion follows from

$$\begin{aligned} \begin{pmatrix} -T_p^\sharp & 1 \end{pmatrix} \begin{pmatrix} p+1 & T_p \\ T_p & p+1 \end{pmatrix} \begin{pmatrix} 1 \\ -T_p^\sharp \end{pmatrix} &= T_p^{\sharp 2} T_p + T_p - 2(p+1)T_p^\sharp \\ &= (T_p^{\sharp 2} - 1)(2T_p^\sharp - T_p). \qquad \square \end{aligned}$$

For general $\Sigma' \subset \Sigma$, we define the morphism of Hecke algebras $t^\flat_{\Sigma',\Sigma} : T^\flat_\Sigma \to T^\flat_{\Sigma'}$ and the morphisms of Hecke modules $m_{\Sigma',\Sigma} : M_\Sigma \to M_{\Sigma'}$ and $m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_\Sigma$ inductively, but we omit the details here.

10.3. Proof of Proposition 10.11

In this section we prove Proposition 10.11 while admitting the following Theorem 10.15. Let p be a prime number, and let $N \geq 1$ be an integer relatively prime to p. Define

$$\begin{aligned} \Gamma(N) &= \operatorname{Ker}\big(\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})\big), \\ \Gamma_{0,*}(p,N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N) \,\middle|\, c \equiv 0 \bmod p \right\}, \\ \tilde{\Gamma}(N) &= \operatorname{Ker}\big(\mathrm{SL}_2(\mathbf{Z}[\tfrac{1}{p}]) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})\big). \end{aligned}$$

In addition, define

$$\begin{aligned} E(N) &= \left\langle A \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} A^{-1} \,\middle|\, A \in \mathrm{SL}_2(\mathbf{Z}) \right\rangle \subset \Gamma(N), \\ \tilde{E}(N) &= \left\langle A \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} A^{-1} \,\middle|\, A \in \mathrm{SL}_2(\mathbf{Z}[\frac{1}{p}]) \right\rangle \subset \tilde{\Gamma}(N). \end{aligned}$$

Let $s_0 : \Gamma_{0,*}(p,N) \to \Gamma(N)$ be the inclusion, and let $s_1 : \Gamma_{0,*}(p,N) \to \Gamma(N)$ be the conjugate $A \mapsto \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} A \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Let $j_0 : \Gamma(N) \to \tilde{\Gamma}(N)$ be the inclusion, and let $j_1 : \Gamma(N) \to \tilde{\Gamma}(N)$ be the conjugate

$A \mapsto \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) A \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$. The amalgamated sum of $s_0, s_1 : \Gamma_{0,*}(p,N) \to \Gamma(N)$ is denoted by $\Gamma(N) *_{\Gamma_{0,*}(p,N)} \Gamma(N)$. For a group Γ, $\Gamma^{\mathrm{ab}} = \Gamma/[\Gamma,\Gamma]$ is its abelianization.

THEOREM 10.15. *Let p be a prime number, and let $N \geq 1$ be an integer relatively prime to p.*

(1) *The homomorphism $\Gamma(N) *_{\Gamma_{0,*}(p,N)} \Gamma(N) \to \tilde{\Gamma}(N)$ defined by the commutative diagram*

$$\begin{tikzcd}
\Gamma(N) \arrow[r, "j_0"] & \tilde{\Gamma}(N) \\
\Gamma_{0,*}(p,N) \arrow[u, "s_0"] \arrow[r, "s_1"] & \Gamma(N) \arrow[u, "j_1"']
\end{tikzcd}$$

is an isomorphism.

(2) $\tilde{\Gamma}(N) = \tilde{E}(N)$.

We do not give a proof of Theorem 10.15 in this book.

COROLLARY 10.16. (1) *$E(N)^{\mathrm{ab}} \to \tilde{\Gamma}(N)^{\mathrm{ab}}$ is surjective.*

(2) *$s_0 \oplus s_1 : \Gamma_{0,*}(p,N)^{\mathrm{ab}} \to (\Gamma(N)^{\mathrm{ab}}/E(N))^2$ is surjective.*

PROOF. (1) Let A be any element of $\mathrm{SL}_2(\mathbf{Z}[\frac{1}{p}])$, and $M = A \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) A^{-1}$. By Theorem 10.15(2), it suffices to show that M is conjugate to an element $E(N)$ by an element of $\tilde{\Gamma}(N)$. If $p^n \equiv 1 \bmod N$, then $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ is conjugate to $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)^{p^{2n}}$ by $\left(\begin{smallmatrix} p^n & 0 \\ 0 & p^{-n} \end{smallmatrix}\right) \in \tilde{\Gamma}(N)$. Thus, M is conjugate to $M^{p^{2n}}$ by $\tilde{\Gamma}(N)$. Therefore, it suffices to show that $M^{p^{2n}} \in E(N)$ for sufficiently large $n > 0$.

Since $(M-1)^2 = 0$ and $M - 1 \in M_2(\mathbf{Z}[\frac{1}{p}])$, we have $M^{p^{2n}} = 1 + p^{2n}(M-1) \in \mathrm{SL}_2(\mathbf{Z})$ for sufficiently large $n > 0$. Since $(M^{p^{2n}} - 1)^2 = 0$, there is an integer $b \in \mathbf{Z}$ such that $M^{p^{2n}}$ is conjugate to $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ by an element of $\mathrm{SL}_2(\mathbf{Z})$. Since $M^{p^{2n}} \equiv 1 \bmod N$, we have $N|b$ and thus $M^{p^{2n}} \in E(N)$.

(2) By Theorem 10.15(1), we obtain an exact sequence

$$\Gamma_{0,*}(p,N)^{\mathrm{ab}} \xrightarrow{s_0 \oplus s_1} \Gamma(N)^{\mathrm{ab}\ 2} \xrightarrow{j_0 - j_1} \tilde{\Gamma}(N)^{\mathrm{ab}} \longrightarrow 0.$$

The assertion is clear from this and (1). □

Let p be a prime number, and let $N \geq 1$ be an integer relatively prime to p. Modular curves $X(N)$ and $X_{0,*}(p,N)$ over $\mathbf{Q}$ are curves over the cyclotomic field $\mathbf{Q}(\zeta_N)$. $s_0, s_1 : X_{0,*}(p,N) \to X(N)$ are defined just as $s_0, s_1 : X_0(Np) \to X_0(N)$. Embed $\mathbf{Q}(\zeta_N)$ into $\mathbf{C}$ by $\zeta_N = \exp\left(\frac{2\pi\sqrt{-1}}{N}\right)$, and let $X(N)^{\mathrm{an}}$ and $X_{0,*}(p,N)^{\mathrm{an}}$ be the compact Riemann surfaces defined by $X(N) \otimes_{\mathbf{Q}(\zeta_N)} \mathbb{C}$ and $X_{0,*}(p,N) \otimes_{\mathbf{Q}(\zeta_N)} \mathbb{C}$, respectively.

PROPOSITION 10.17. *Let p be a prime number, and let $N \geq 1$ be an integer relatively prime to p. Then,*

$$s_{0*} \oplus s_{1*} : H_1(X_{0,*}(p,N)^{\mathrm{an}}, \mathbf{Z}) \longrightarrow H_1(X(N)^{\mathrm{an}}, \mathbf{Z})^2$$

is surjective.

PROOF. If $N = 1, 2$, then the genus of $X(N)$ is 0, and thus we may assume $N \geq 3$. If $N \geq 3$, then, by Lemma 8.37, $\Gamma(N)$ acts freely on the upper half-plane $H = \{\tau \in \mathbf{C} \mid \operatorname{Im} \tau > 0\}$, and we have $\Gamma(N) \backslash H = Y(N)^{\mathrm{an}}$ and $\Gamma_{0,*}(p,N) \backslash H = Y_{0,*}(p,N)^{\mathrm{an}}$. Thus, we obtain isomorphisms of fundamental groups $\Gamma(N) \to \pi_1(Y(N)^{\mathrm{an}})$ and $\Gamma_{0,*}(p,N) \to \pi_1(Y_{0,*}(p,N)^{\mathrm{an}})$. Moreover, the inertia groups at the cusps of $Y(N)$ are conjugate to $\langle\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)\rangle = \Gamma(N) \cap \langle\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\rangle$, these isomorphisms define a commutative diagram

$$\begin{tikzcd}
\Gamma_{0,*}(p,N)^{\mathrm{ab}} \arrow[r, "s_0 \oplus s_1"] \arrow[d] & (\Gamma(N)^{\mathrm{ab}}/E(N))^2 \arrow[d] \\
H_1(X_{0,*}(p,N)^{\mathrm{an}}, \mathbf{Z}) \arrow[r, "s_{0*} \oplus s_{1*}"] & H_1(X(N)^{\mathrm{an}}, \mathbf{Z})^2.
\end{tikzcd}$$

The left vertical arrow is surjective, and the right vertical arrow is an isomorphism. Thus, the assertion follows immediately from Corollary 10.16(2). □

COROLLARY 10.18. *Let p be a prime number, and let $N \geq 1$ be an integer relatively prime to p. Then,*

$$s_{0*} \oplus s_{1*} : H_1(X_{1,0}(N,p)^{\mathrm{an}}, \mathbf{Z}) \longrightarrow H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z})^2$$

is surjective.

This is a more precise version of an analog of Corollary 9.30(2).

PROOF. Consider the subgroups $\Gamma(N) \subset \Gamma_1(N)$ of $\mathrm{SL}_2(\mathbf{Z})$. By the isomorphisms of Riemann surfaces (8.47) and (8.40), the homomorphism $H_1(Y(N)^{\mathrm{an}}, \mathbf{Z}) \to H_1(Y_1(N)^{\mathrm{an}}, \mathbf{Z})$ is identified with that of abelianizations $\Gamma(N)^{\mathrm{ab}} \to \Gamma_1(N)^{\mathrm{ab}}$. $H_1(X(N)^{\mathrm{an}}, \mathbf{Z})$ and $H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z})$ are the quotients by the images of inertia groups of $H_1(Y(N)^{\mathrm{an}}, \mathbf{Z})$ and $H_1(Y_1(N)^{\mathrm{an}}, \mathbf{Z})$, respectively. The cokernel of $\Gamma(N) \to \Gamma_1(N)$ is generated by the images of the inertia group $\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ at the cusp, and $H_1(X(N)^{\mathrm{an}}, \mathbf{Z}) \to H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z})$ is surjective. Hence, the assertion follows from Proposition 10.17 and the commutative diagram

$$\begin{tikzcd}
H_1(X_{*,0}(N,p)^{\mathrm{an}}, \mathbf{Z}) \arrow[r] \arrow[d] & H_1(X(N)^{\mathrm{an}}, \mathbf{Z}) \arrow[d] \\
H_1(X_{1,0}(N,p)^{\mathrm{an}}, \mathbf{Z}) \arrow[r] & H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z}).
\end{tikzcd}$$

□

PROPOSITION 10.19. *Let p be a prime number, and let $N \geq 4$ be an integer relatively prime to p. Then,*

$$\begin{aligned} H_1(Y_{1,0}(N,p^2)^{\mathrm{an}}, \mathbf{Z}) &\xrightarrow{(t_{1*}, -t_{0*})} H_1(Y_{1,0}(N,p)^{\mathrm{an}}, \mathbf{Z})^2 \\ &\xrightarrow{s_{0*}+s_{1*}} H_1(Y_1(N)^{\mathrm{an}}, \mathbf{Z}) \longrightarrow 0 \end{aligned} \tag{10.12}$$

is an exact sequence of $\mathbf{Z}$-modules.

PROOF. By the assumption $N \geq 4$, $Y_1(N)$ is a fine moduli scheme. Similarly to Lemma 9.35(3), the commutative diagram of finite étale morphisms of curves

(10.13)
$$\begin{tikzcd}
Y_{1,0}(N,p^2) \amalg Y_{1,0}(N,p) \arrow[r, "{(t_1, \mathrm{id})}"] \arrow[d, "{(t_0, w \circ t_0)}"'] & Y_{1,0}(N,p) \arrow[d, "s_0"] \\
Y_{1,0}(N,p) \arrow[r, "s_1"] & Y_1(N)
\end{tikzcd}$$

is Cartesian. Therefore, the commutative diagram

(10.14)
$$\begin{tikzcd}
\pi_1(Y_{1,0}(N,p^2)) \arrow[r, "t_{1*}"] \arrow[d, "t_{0*}"'] & \pi_1(Y_{1,0}(N,p)) \arrow[d, "s_{0*}"] \\
\pi_1(Y_{1,0}(N,p)) \arrow[r, "s_{1*}"] & \pi_1(Y_1(N))
\end{tikzcd}$$

induces an isomorphism $\pi_1(Y_{1,0}(N,p)) *_{\pi_1(Y_{1,0}(N,p^2))} \pi_1(Y_{1,0}(N,p)) \to \pi_1(Y_1(N))$. We obtain the exact sequence (10.12) from this. □

LEMMA 10.20. *Let $N \geq 5$ be an integer, and let p be a prime number that does not divide N. The action of the Hecke operator T_p on the kernel of $H_1(Y_1(N)^{\mathrm{an}}, \mathbf{Z}) \to H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z})$ is multiplication by $\langle p \rangle + p$.*

PROOF. Let $Z_1(N) = X_1(N)^{\mathrm{an}} - Y_1(N)^{\mathrm{an}}$ be the set of cusps. Then, we have an exact sequence of $T_1(N)_{\mathbf{Z}}$-modules

$$\mathbf{Z}^{Z_1(N)} \longrightarrow H_1(Y_1(N)^{\mathrm{an}}, \mathbf{Z}) \longrightarrow H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z}) \longrightarrow 0.$$

Thus, it suffices to study the action of the Hecke operator T_p on the free $\mathbf{Z}$-module $\mathbf{Z}^{Z_1(N)}$ generated by the cusps.

By the assumption $N \geq 5$, $X_1(N)$ is a fine moduli scheme of generalized elliptic curves with level structure. Thus, $Z_1(N)$ is identified with the set

$$\left\{\begin{array}{l}\text{isomorphism classes of pairs } (P_d, P), \text{ where } P_d\ (d \mid N) \text{ is} \\ \text{the Néron } d\text{-gon over } \mathbf{C}, \text{ and } P \text{ is a point of exact order} \\ N \text{ of the smooth part } P_d^{\mathrm{sm}} \simeq \mathbf{G}_m \times \mathbf{Z}/d\mathbf{Z} \text{ such that } \langle P \rangle \\ \text{intersects with all the connected component of } P_d^{\mathrm{sm}}\end{array}\right\}.$$

Similarly, $Z_{1,0}(N,p) = X_{1,0}(N,p)^{\mathrm{an}} - Y_{1,0}(N,p)^{\mathrm{an}}$ is identified with the set

$$\left\{\begin{array}{l}\text{isomorphism classes of triples } (P_d, P, C), \text{ where } P_d \\ (d \mid Np) \text{ is the Néron } d\text{-gon over } \mathbf{C},\ P \text{ is a point of ex-} \\ \text{act order } N \text{ of the smooth part } P_d^{\mathrm{sm}} \simeq \mathbf{G}_m \times \mathbf{Z}/d\mathbf{Z}, \text{ and} \\ C \subset P_d^{\mathrm{sm}} \text{ is a cyclic subgroup of order } p \text{ such that } \langle P \rangle + C \\ \text{intersects with all the connected component of } P_d^{\mathrm{sm}}\end{array}\right\}.$$

The mappings $s, t : Z_{1,0}(N,p) \to Z_1(N)$ are described as follows. For a triple (P_d, P, C), let Q be the Néron polygon obtained by contracting the irreducible components of P_d that do not intersect with $\langle P \rangle$. Then we have $s(P_d, P, C) = (Q, \text{image of } P)$. Also we have $t(P_d, P, C) = (P_d/C, \text{image of } P)$.

The inverse image of the point (P_d, P) by $s : Z_{1,0}(N,p) \to Z_1(N)$ consists of two points $(P_d, P, \mu_p \times 1)$ and $(P_{dp}, P, 1 \times d\mathbf{Z}/dp\mathbf{Z})$, and their ramification indices are 1 and p, respectively. Here, we identified $P_d^{\mathrm{sm}} = \mathbf{G}_m \times \mathbf{Z}/d\mathbf{Z}$ with the subgroup of $P_{dp}^{\mathrm{sm}} = \mathbf{G}_m \times \mathbf{Z}/dp\mathbf{Z}$ through the multiplication-by-p mapping $\mathbf{Z}/d\mathbf{Z} \to \mathbf{Z}/dp\mathbf{Z}$. Furthermore, the images of $(P_d, P, \mu_p \times 1)$ and $(P_{dp}, P, 1 \times d\mathbf{Z}/dp\mathbf{Z})$ by $t : Z_{1,0}(N,p) \to Z_1(N)$ are (P_d, pP) and (P_d, P), respectively. Hence, the image of $[(P_d, P)] \in \mathbf{Z}^{Z_1(N)}$ by $T_p = t_* \circ s^*$ is $[(P_d, pP)] + p[(P_d, P)] = (\langle p \rangle + p)[(P_d, P)]$. □

LEMMA 10.21. *Let $N \geq 1$ be an integer, and let p be a prime number that does not divide N. The action of the Hecke operator T_p on* $\mathrm{Coker}(H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z}) \to H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}))$ *is the multiplication by $p+1$.*

PROOF. $X_0(N)$ is the quotient of $X_1(N)$ by $(\mathbf{Z}/N\mathbf{Z})^\times$ acting as the diamond operators. Since $H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z})$ and $H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z})$ are the abelianizations of the fundamental groups $\pi_1(X_1(N)^{\mathrm{an}})$ and $\pi_1(X_0(N)^{\mathrm{an}})$, $\mathrm{Coker}(H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z}) \to H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}))$ is identified with the quotient of $(\mathbf{Z}/N\mathbf{Z})^\times$ corresponding to the maximal unramified intermediate coverings of $X_1(N) \to X_0(N)$. Since the morphisms $s, t : X_{1,0}(N, p) \to X_1(N)$ are compatible with the action of $(\mathbf{Z}/N\mathbf{Z})^\times$, the induced mappings $s_*, t_* : \mathrm{Coker}(H_1(X_{1,0}(N,p)^{\mathrm{an}}, \mathbf{Z}) \to H_1(X_0(Np)^{\mathrm{an}}, \mathbf{Z})) \to \mathrm{Coker}(H_1(X_1(N)^{\mathrm{an}}, \mathbf{Z}) \to H_1(X_0(N)^{\mathrm{an}}, \mathbf{Z}))$ are equal. Thus, we have $T_p = t_* \circ s^* = s_* \circ s^* = \deg s = p+1$. □

Let $\mathcal{O}$ be the ring of integers of a finite extension K of $\mathbf{Q}_\ell$, let $M \geq 1$ be an integer, and let $\mathcal{O}[T_p, p \nmid M]$ be the ring of polynomials with infinite number of variables. Let $\mathfrak{m}$ be a maximal ideal of $\mathcal{O}[T_p, p \nmid M]$ such that the residue field $\mathbf{F} = \mathcal{O}[T_p, p \nmid M]/\mathfrak{m}$ is a finite field. If there do not exist characters $\alpha, \beta : (\mathbf{Z}/M\mathbf{Z})^\times \to \mathbf{F}^\times$ such that $T_p \equiv \alpha(p) + \beta(p) \bmod \mathfrak{m}$ for all $p \nmid M$, then $\mathfrak{m}$ is said to be *non-Eisenstein*. For a factor M' of M, $H_1(X_0(M')^{\mathrm{an}}, \mathcal{O})$ and $H_1(X_1(M')^{\mathrm{an}}, \mathcal{O})$ are $\mathcal{O}[T_p, p \nmid M]$-modules, and for a maximal ideal $\mathfrak{m}$, the localizations $H_1(X_0(M')^{\mathrm{an}}, \mathcal{O})_\mathfrak{m}$ and $H_1(X_1(M')^{\mathrm{an}}, \mathcal{O})_\mathfrak{m}$ at $\mathfrak{m}$ are defined.

PROPOSITION 10.22. *Let p be a prime number, and let $N \geq 1$ be an integer relatively prime to p. Let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of the polynomial ring $\mathcal{O}[T_q, q \nmid Np^2]$. Then,*

$$(10.15) \quad s_{0*} \oplus s_{1*} \oplus s_{2*} : H_1(X_0(Np^2)^{\mathrm{an}}, \mathcal{O})_\mathfrak{m} \longrightarrow H_1(X_0(N)^{\mathrm{an}}, \mathcal{O})^3_\mathfrak{m}$$

is surjective.

PROOF. If $N \leq 4$, then the genus of $X_1(N)$ is 0, and thus we may assume $N \geq 5$. Consider the following diagram.

$$\begin{tikzcd}
 & 0 \arrow[d] \\
H_1(X_{1,0}(N,p^2)^{\mathrm{an}},\mathcal{O})_{\mathfrak{m}} \arrow[r, "s_{0*}\oplus s_{1*}\oplus s_{2*}"] \arrow[d, "t_{1*}-t_{0*}"'] & H_1(X_1(N)^{\mathrm{an}},\mathcal{O})^3_{\mathfrak{m}} \arrow[d, "\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}"] \\
H_1(X_{1,0}(N,p)^{\mathrm{an}},\mathcal{O})^2_{\mathfrak{m}} \arrow[r, "(s_{0*}\oplus s_{1*})^2"] \arrow[d, "s_{0*}+s_{1*}"'] & H_1(X_1(N)^{\mathrm{an}},\mathcal{O})^4_{\mathfrak{m}} \arrow[d, "\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}"] \\
H_1(X_1(N)^{\mathrm{an}},\mathcal{O})_{\mathfrak{m}} \arrow[r, equal] \arrow[d] & H_1(X_1(N)^{\mathrm{an}},\mathcal{O})_{\mathfrak{m}} \arrow[d] \\
0 & 0.
\end{tikzcd} \tag{10.16}$$

The right column is clearly exact. Since $\mathfrak{m}$ is non-Eisenstein, we may replace X by Y in the left vertical column by Lemma 10.20. Thus, by Proposition 10.19, the left column is exact. Furthermore, by Corollary 10.18, the middle horizontal arrow is surjective. Thus, by the snake lemma, the upper horizontal arrow is also surjective.

Consider the commutative diagram

$$\begin{tikzcd}
H_1(X_{1,0}(N,p^2)^{\mathrm{an}},\mathcal{O})_{\mathfrak{m}} \arrow[r, "s_{0*}\oplus s_{1*}\oplus s_{2*}"] \arrow[d] & H_1(X_1(N)^{\mathrm{an}},\mathcal{O})^3_{\mathfrak{m}} \arrow[d] \\
H_1(X_0(Np^2)^{\mathrm{an}},\mathcal{O})_{\mathfrak{m}} \arrow[r, "s_{0*}\oplus s_{1*}\oplus s_{2*}"] & H_1(X_0(N)^{\mathrm{an}},\mathcal{O})^3_{\mathfrak{m}}.
\end{tikzcd} \tag{10.17}$$

Since $\mathfrak{m}$ is non-Eisenstein, the right vertical arrow is surjective by Lemma 10.21. Thus, the lower horizontal arrow is also surjective. □

PROOF OF PROPOSITION 10.11. By Proposition 9.26, the maximal ideal $\mathfrak{m}_\Sigma$ is non-Eisenstein. Thus, the inverse image of $\mathfrak{m}_\Sigma$ by $\mathcal{O}[T_p, p \nmid M] \to T(N_\Sigma)_{\mathcal{O}}$ is also non-Eisenstein. In the case of $p \neq \ell$, the assertion follows immediately from Proposition 10.22. The case $p = \ell$ is similar, but we omit the details. □

10.4. Deformation rings and group rings

As a preliminary for the construction of the family of liftings of $(R, M) = (R_\varnothing, M_\varnothing)$ in the next section, we study the relationship between deformation rings and group rings.

Let $\widetilde{\mathcal{Q}}$ be the set of all the prime numbers satisfying the conditions

$$q \notin S_{\bar{\rho}} \quad q \neq \ell \quad \text{and} \quad \operatorname{Tr} \bar{\rho}(\varphi_q) \not\equiv \pm(q+1). \tag{10.18}$$

The condition $\operatorname{Tr} \bar{\rho}(\varphi_q) \not\equiv \pm(q+1)$ can also be stated as $(\operatorname{Tr} \bar{\rho}(\varphi_q))^2 \not\equiv (q+1)^2$. For $q \in \widetilde{\mathcal{Q}}$, let $\bar{\alpha}_q$ and $\bar{\beta}_q$ be the eigenvalues of $\bar{\rho}(\varphi_q)$. Since $q \equiv \bar{\alpha}_q \bar{\beta}_q$, the condition $\bar{\alpha}_q \bar{\beta}_q \pm (\bar{\alpha}_q + \bar{\beta}_q) + 1 \neq 0$ in (10.18) is equivalent to the condition $\bar{\alpha}_q \neq \pm 1$ and $\bar{\beta}_q \neq \pm 1$, or $\bar{\alpha}_q / \bar{\beta}_q \neq q^{\pm 1}$. Thus, if $q \equiv 1 \bmod \ell$, we have $\bar{\alpha}_q \neq \bar{\beta}_q$. In what follows, we assume that $\bar{\alpha}_q$ and $\bar{\beta}_q$ belong to $\mathbf{F}$ for each $q \in \widetilde{\mathcal{Q}}$ after replacing K by its unramified quadratic extension if necessary.

For $q \in \widetilde{\mathcal{Q}}$, let Δ_q be the maximal ℓth power quotient of $(\mathbf{Z}/q\mathbf{Z})^\times$ identified with $\operatorname{Gal}(\mathbf{Q}_q(\zeta_q)/\mathbf{Q}_q)$. If $q \not\equiv 1 \bmod \ell$, then we have $\Delta_q = 1$. We identify Δ_q with a quotient of the inertia group I_q through the surjection $I_q \to \operatorname{Gal}(\mathbf{Q}_q(\zeta_q)/\mathbf{Q}_q) = (\mathbf{Z}/q\mathbf{Z})^\times$. Δ_q is identified with the maximal ℓth power quotient of the image in the abelianization $\operatorname{Im}(I_q \to G_{\mathbf{Q}_q}^{\mathrm{ab}})$.

The condition $\operatorname{Tr} \bar{\rho}(\varphi_q) \not\equiv \pm(q+1)$ is made for the following proposition.

Proposition 10.23. *Let $q \in \widetilde{\mathcal{Q}}$, and let R be a profinitely generated complete local $\mathcal{O}$-algebra. Let $\mathbf{F}_R$ be the residue field of R. Let $\rho_q : G_{\mathbf{Q}_q} \to \mathrm{GL}_2(R)$ be a lifting of the restriction of $\bar{\rho}$ to $G_{\mathbf{Q}_q}$.*

1. *Suppose $\bar{\alpha}_q \neq \bar{\beta}_q$. There is a unique pair of characters $\alpha_q, \beta_q : G_{\mathbf{Q}_q} \to R^\times$ such that ρ_q is isomorphic to the direct sum $\alpha_q \oplus \beta_q$, and the composition $G_{\mathbf{Q}_q} \to R^\times \to \mathbf{F}_R^\times$ are unramified characters whose values at φ_q are determined by $\bar{\alpha}_q$ and $\bar{\beta}_q$, respectively. The restriction of the characters $\alpha_q, \beta_q : G_{\mathbf{Q}_q}^{\mathrm{ab}} \to R^\times$ to the inertia group I_q induces characters $\Delta_q \to R^\times$ of the quotient group Δ_q.*
2. *If $q \not\equiv 1 \bmod \ell$, then ρ_q is unramified.*

Proof. Let $F \in G_{\mathbf{Q}_p}$ be a lifting of the Frobenius substitution $\varphi_q \in G_{\mathbf{F}_q}$. Replacing the basis of R^2 if necessary, we may assume $\rho_q(F) = P = \begin{pmatrix} \tilde{\alpha} & 0 \\ 0 & \tilde{\beta} \end{pmatrix}$. If $\sigma \in I_q$ is any element of the inertia group, we have $P\rho_q(\sigma)P^{-1} = \rho_q(\sigma)^q$ and $\rho_q(\sigma) \equiv 1 \bmod \mathfrak{m}_R$. Thus, if $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ $(a, b, c, d \in \mathfrak{m}_R)$ satisfies $PAP^{-1} = (1+A)^q - 1$, it suffices to show that $b = c = 0$. Since $PAP^{-1} = (1+A)^q - 1$, there exist polynomials f and g of four variables with $\mathbf{Z}$ coefficients whose constant terms are 0 that satisfy $\tilde{\alpha}\tilde{\beta}^{-1}b = (q + f(a,b,c,d))b$ and $\tilde{\beta}\tilde{\alpha}^{-1}c = (q + g(a,b,c,d))c$. By assumption, we have $\tilde{\alpha}\tilde{\beta}^{-1}$ and $\tilde{\beta}\tilde{\alpha}^{-1} \not\equiv q$ and $f(a,b,c,d) \equiv g(a,b,c,d) \equiv 0 \bmod \mathfrak{m}_R$. Thus, we have $b = c = 0$.

As above, we identify Δ_q with the maximal ℓth power quotient of the image in the abelianization $\mathrm{Im}(I_q \to G^{\mathrm{ab}}_{\mathbf{Q}_q})$. Since $1 + \mathfrak{m}_R M_2(R) \subset \mathrm{GL}_2(R)$ is a pro-ℓ group, the restriction of α_q, β_q to I_q passes through Δ_q.

(2) We first show it in the case $\bar{\alpha}_q \neq \bar{\beta}_q$. From (1) we see that there exist characters $\alpha_q, \beta_q : G^{\mathrm{ab}}_{\mathbf{Q}_q} \to R^\times$ satisfying $\rho_q \simeq \alpha_q \oplus \beta_q$. By the assumption $q \not\equiv 1 \bmod \ell$, the image Δ_q of the inertia group is trivial, and α_q and β_q are unramified.

We show it in the case $\bar{\alpha}_q = \bar{\beta}_q$. We show that the image $\rho_q(I_q)$ of the inertia group I_q is trivial. Replacing R by $R/\mathfrak{m}_R^n$ if necessary, we may assume R is finite. Suppose the order of the image $\rho_q(I_q) \subset 1 + \mathfrak{m}_R M_2(R)$ is ℓ^m. We want to show $m = 0$. Since $\ell \neq q$, $\rho_q(I_q)$ is a cyclic group of order ℓ^m. Let A be a generator of the cyclic group $\rho_q(I_q)$. Suppose $F \in G_{\mathbf{Q}_q}$ is a lifting of $\varphi_q \in G_{\mathbf{Q}_q}$. Let $\tilde{\alpha} \in R$ be a root of unity of order prime to ℓ that satisfy $\tilde{\alpha} \equiv \bar{\alpha}_q \bmod \mathfrak{m}_R$. If we let $\rho(F) = \tilde{\alpha}P$, we have $PAP^{-1} = A^q$. If the order of P is N, then we have $A^{q^N} = A$, and thus $q^N \equiv 1 \bmod \ell^m$. Since the only eigenvalue of $P \bmod \mathfrak{m}_R$ is 1, N is a power of ℓ, and we have $q^N \equiv q \bmod \ell$. Since $q \not\equiv 1 \bmod \ell$, we conclude that $m = 0$. □

As we noted above, if $q \equiv 1 \bmod \ell$, we have $\bar{\alpha}_q \neq \bar{\beta}_q$, and thus the condition of Proposition 10.23(1) is satisfied in this case.

COROLLARY 10.24. *The notation is as in Proposition* 10.23. *Assume furthermore that* $q \equiv 1 \bmod \ell$ *and that the restriction of* $\det \rho_q$ *to the inertia group* I_q *is the* ℓ*-adic cyclotomic character. Then* ρ_q *is unramified if and only if* $a_q|_{I_q}$ *is trivial.*

PROOF. Since $q \neq \ell$, $\det \rho_q = \alpha_q\beta_q$ is unramified and we have $\alpha|_{I_q} = \beta|_{I_q}^{-1}$. □

Let $\mathcal{Q} = \{q \in \tilde{\mathcal{Q}} \mid q \equiv 1 \bmod \ell\}$. In what follows, we identify a finite subset $Q \subset \mathcal{Q}$ with the integer $\prod_{q \in Q} q$. For a finite subset Q in $\mathcal{Q}$, define $\Delta_Q = \prod_{q \in Q} \Delta_q$. Through the identification $(\mathbf{Z}/Q\mathbf{Z})^\times =$

$\prod_{q\in Q}(\mathbf{Z}/q\mathbf{Z})^\times$, we identify Δ_Q with a quotient group of $(\mathbf{Z}/Q\mathbf{Z})^\times$. For each $q \in \mathcal{Q}$, choose one of two eigenvalues of $\bar{\rho}(\varphi_q)$ and denote it by $\bar{\alpha}_q \in \mathbf{F}^\times$. We define a ring homomorphism

$$\mathcal{O}[\Delta_Q] \longrightarrow R_Q. \tag{10.19}$$

Let $\rho_Q : G_{\mathbf{Q}} \to \mathrm{GL}_2(R_Q)$ be the universal representation. For each $q \in Q$, apply Proposition 10.23(1) to the restriction $\rho_q : G_{\mathbf{Q}_q} \to \mathrm{GL}_2(R_Q)$ of ρ_Q to the decomposition group $G_{\mathbf{Q}_q}$, and we define a character $\alpha_q : G^{\mathrm{ab}}_{\mathbf{Q}_q} \to R_Q^\times$. By Proposition 10.23(1), the character α_q to the inertia group I_q induces a character $\Delta_q \to R_Q^\times$. Define $\mathcal{O}[\Delta_Q] \to R_Q$ as the ring homomorphism induced by the product of these characters, $\Delta_Q \to R_Q^\times$.

LEMMA 10.25. *Let Q be a finite set of prime numbers in $\mathcal{Q} = \{q \in \widetilde{\mathcal{Q}} \mid q \equiv 1 \bmod \ell\}$, and let $\mathcal{O}[\Delta_Q] \to \mathcal{O}$ be the augmentation morphism. Then, the diagram*

$$\begin{tikzcd}
\mathcal{O}[\Delta_Q] \arrow[r] \arrow[d] & R_Q \arrow[d] \\
\mathcal{O} \arrow[r] & R_\varnothing
\end{tikzcd}$$

is commutative, and the induced morphism $R_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} \to R_\varnothing$ is an isomorphism.

PROOF. Since the universal representation $\rho_\varnothing : G_{\mathbf{Q}} \to \mathrm{GL}_2(R_\varnothing)$ is unramified at Q, the commutativity of the diagram is clear from the definition of $\mathcal{O}[\Delta_Q] \to R_Q$. If ρ is a lifting of $\bar{\rho}$ of type $\mathcal{D}_Q$, then, by Corollary 10.24, ρ is a lifting of type $\mathcal{D}$ if and only if $\alpha_q : G_{\mathbf{Q}_q} \to R^\times$ is unramified for any $q \in Q$. Thus, $R_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O}$ represents the functor $\mathrm{Def}_{\bar{\rho},\mathcal{D}_\varnothing}$ over $\mathcal{O}$. Hence, $R_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} \to R_\varnothing$ is an isomorphism. □

QUESTION. Let $\widetilde{Q}$ be a finite subset $\widetilde{\mathcal{Q}}$, and let $Q = \widetilde{Q} \cap \mathcal{Q}$. Show that the natural morphism $R_{\widetilde{Q}} \to R_Q$ is an isomorphism. (*Hint*: You may prove this similarly to the proof of Lemma 10.25.)

PROPOSITION 10.26. *There exist infinitely many odd prime numbers $q \in \widetilde{\mathcal{Q}}$ such that $q \not\equiv 1 \bmod \ell$.*

PROOF. $\det \bar{\rho}$ is the mod ℓ cyclotomic character and is of even order. Thus, by Theorem 3.1 and Lemma 9.51, the assertion is now reduced to the following lemma of group theory. □

LEMMA 10.27. *Let* $\mathbf{F}$ *be a finite field of characteristic* $\ell \geq 3$, *let* $\rho : G \to \mathrm{GL}_2(\mathbf{F})$ *be an absolutely irreducible representation of a finite group* G, *and let* $\chi : G \to \mathbf{F}^\times$ *be a character. Suppose the order of* χ *is an even integer* $2d$. *In case* $2d = 2$, *we assume further that the restriction of* ρ *to* $H = \operatorname{Ker}\chi$ *is absolutely irreducible. Then, there exists an element* σ *of* G *satisfying the condition*

$$\chi(\sigma) \neq 1 \ \ \textit{and} \ \ \frac{(\operatorname{Tr}\rho(\sigma))^2}{\det\rho(\sigma)} \neq \frac{(1+\chi(\sigma))^2}{\chi(\sigma)}. \tag{10.20}$$

We deduce the above lemma from the following theorem.

THEOREM 10.28. *Let* ℓ *be a prime number, let* $\overline{\mathbf{F}}_\ell$ *be an algebraic closure of* $\mathbf{F}_\ell$, *and let* $G \subset \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ *be a finite subgroup. Suppose* $V = \overline{\mathbf{F}}_\ell^2$ *is absolutely irreducible as a representation of* G. *Then, the image* $\overline{G}$ *of* G *in* $PGL_2(\overline{\mathbf{F}}_\ell) = \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)/\overline{\mathbf{F}}_\ell^\times$ *satisfies one of the following conditions* (i), (ii), *and* (iii).

(i) *There exists a finite extension* $\mathbf{F}$ *of* $\mathbf{F}_\ell$ *such that* $\overline{G}$ *is conjugate to either* $PGL_2(\mathbf{F})$ *or* $PSL_2(\mathbf{F})$.

(ii) $\overline{G}$ *is isomorphic to the symmetric group* $\mathfrak{S}_4$, *the alternating group* $\mathfrak{A}_4$, *or* $\mathfrak{A}_5$.

(iii) $\overline{G}$ *is isomorphic to the dihedral group* D_{2n} *of order* $2n$ *with* n *and* ℓ *relatively prime to each other.*

We omit the proof of Theorem 10.28.

PROOF OF LEMMA 10.27. We prove it by contradiction. Let $\alpha(\sigma), \beta(\sigma)$ be eigenvalues of $\rho(\sigma)$. Then the condition $\frac{(\alpha(\sigma)+\beta(\sigma))^2}{\alpha(\sigma)\beta(\sigma)} \neq \frac{(1+\chi(\sigma))^2}{\chi(\sigma)}$ is equivalent to $\frac{\alpha(\sigma)}{\beta(\sigma)} + \frac{\beta(\sigma)}{\alpha(\sigma)} \neq \chi(\sigma) + \frac{1}{\chi(\sigma)}$, and in turn equivalent to $\frac{\alpha(\sigma)}{\beta(\sigma)} \neq \chi(\sigma)^{\pm 1}$. Suppose the negation of condition (10.20), that is

$$\text{if } \sigma \in G, \text{ then } \chi(\sigma) = 1 \text{ or } \frac{\alpha(\sigma)}{\beta(\sigma)} = \chi(\sigma)^{\pm 1} \tag{10.21}$$

holds, and we derive a contradiction to the assumption of Lemma 10.27.

Let $Z = \{\sigma \in G \mid \rho(\sigma) \text{ is scalar matrix}\}$. By (10.21), we have $Z \subset \operatorname{Ker}\chi = H$. Thus, we have $\operatorname{Ker}\rho \subset Z \subset \operatorname{Ker}\chi$, and replacing G by $\rho(G)$, we may assume $G \subset \mathrm{GL}_2(\mathbf{F})$.

Take an element $\sigma \in G$ such that $\chi(\sigma)$ is a generator of $\chi(G)$. Let $\overline{} : G \to \overline{G} = G/Z$ be the natural surjection, and let $\overline{H} = H/Z$. We show that $\overline{G} = \langle\bar{\sigma}\rangle \ltimes \overline{H}$ and $\overline{H}$ is an abelian group. By (10.21), replacing $\mathbf{F}$ by its quadratic extension and changing bases if necessary, we may assume $\sigma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & \chi(\sigma) \end{smallmatrix}\right) \bmod \mathbf{F}^\times$. From this $\overline{G} = \langle\sigma\rangle \ltimes \overline{H}$ follows immediately. Suppose $\tau \in H$. Since we have $\chi(\sigma^d\tau) = \chi(\sigma)^d = -1$, the eigenvalues of $\sigma^d\tau$ is of the form $\alpha, -\alpha$, and $(\sigma^d\tau)^2 \in Z$. Hence, we have $\tau^{-1} \equiv \sigma^d\tau\sigma^{-d} \bmod Z$. Thus, $\tau \mapsto \tau^{-1}$ defines an automorphism of $\overline{H} = H/Z$, $\overline{H}$ is an abelian group.

Since $\overline{G} = \langle\bar\sigma\rangle \ltimes \overline{H}$, the order of $\bar\sigma$ is even, and $\overline{H}$ is abelian, it follows from Theorem 10.28 that $\overline{G} \subset PGL_2(\mathbf{F})$ satisfies condition (iii) of Theorem 10.28. Suppose $\overline{G}$ is a dihedral group of order $2n$ $(\ell \nmid n)$. Since $(\overline{G}^{\mathrm{ab}})^2 = 1$, the order of χ is 2. Since the order of any element of $\overline{G} - \overline{H}$ is 2, $\overline{H}$ is a cyclic group of order n. Thus, H is an abelian group of order prime to ℓ, and the restriction of ρ to H is absolutely reducible, which is a contradiction. ☐

10.5. Family of liftings

$\mathcal{Q} = \{\mathfrak{q} \in \widetilde{\mathcal{Q}} \mid q \equiv 1 \bmod \ell\}$ is the set of all the prime numbers q satisfying the condition

$$(10.22) \qquad q \notin S_{\bar\rho}, \quad q \equiv 1 \bmod \ell \quad \text{and} \quad \operatorname{Tr}\bar\rho(\varphi_q) \not\equiv \pm 2.$$

Condition (10.22) is the same as condition (5.19). Choose a prime number $q' \in \widetilde{\mathcal{Q}} - \mathcal{Q}$ satisfying the condition of Proposition 10.26, and fix it once and for all. For a finite set Q of prime numbers in $\mathcal{Q}$, we define variants $T_Q^\natural$, $M_Q^\natural$ of the full Hecke algebra $T_Q^\flat$ and the Hecke module M_Q and a homomorphism $f_Q^\natural : R_Q \to T_Q^\natural$ from the deformation ring to the Hecke algebra, and we will show that these form a family of liftings.

As in the previous section, for each $q \in \mathcal{Q}$, choose an eigenvalue of $\bar\rho(\varphi_q)$ and denote it by $\bar\alpha_q$. By Hensel's lemma, for each $q \in \mathcal{Q}$, there exists a unique root in $T_\varnothing^\flat$ of $U^2 - T_qU + q = 0$ whose image in $\mathbf{F}$ is $\bar\alpha_q$. We write it $T_q^\sharp$. We identify a finite set $Q \subset \mathcal{Q}$ with the integer $\prod_{q\in Q} q$. In what follows, the Hecke algebra $T_{0,1}(N_\varnothing, Qq'^2)_{\mathbf{Z}} = \mathbf{Z}[T_n\ (n \geq 1), \langle a\rangle (a \in (\mathbf{Z}/Qq'^2\mathbf{Z})^\times)] \subset \operatorname{End} J_{0,1}(N_\varnothing, Qq'^2)$ will be written by $T(N_\varnothing, Qq'^2)_{\mathbf{Z}}$. Let $T(N_\varnothing, Qq'^2)_{\mathcal{O}} = T(N_\varnothing, Qq'^2)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathcal{O}$. Just as Proposition 10.6, we show the following.

PROPOSITION 10.29. *Let Q be a finite subset of $\mathcal{Q}$, and let q' be a prime number satisfying the condition in Proposition 10.26. Then there exists a unique ring homomorphism* $\tilde t_{\varnothing,Q} : T(N_\varnothing, Qq'^2)_{\mathcal{O}} \to T_\varnothing^\flat$

satisfying the conditions

$$\tilde{t}_{\varnothing,Q}(T_p) = \begin{cases} T_p & \text{if } p \notin Q \cup \{q'\}, \\ T_q^{\sharp} & \text{if } p = q \in Q, \\ 0 & \text{if } p = q', \end{cases} \tag{10.23}$$

$$\tilde{t}_{\varnothing,Q}(\langle a \rangle) = 1 \qquad a \in (\mathbf{Z}/Qq'^2\mathbf{Z})^{\times}. \tag{10.24}$$

PROOF. The uniqueness is clear. We show the existence. The natural mapping $X_{0,1}(N_\varnothing, Qq'^2) \to X_0(N_\varnothing Qq'^2)$ induces a ring homomorphism $T(N_\varnothing, Qq'^2)_{\mathcal{O}} \to T(N_\varnothing Qq'^2)_{\mathcal{O}}$. For a prime number p, the image of T_p is T_p, and for $a \in (\mathbf{Z}/Qq'^2\mathbf{Z})^{\times}$, the image of $\langle a \rangle$ is 1. Thus, it suffices to give a ring homomorphism $T(N_\varnothing Qq'^2)_{\mathcal{O}} \to T_\varnothing^{\flat}$ satisfying condition (10.23). For $q \in Q \cup \{q'\}$, we define a polynomial $P_q(U) \in T(N_\varnothing)[U]$ as in the proof of Proposition 10.1 by

$$P_q(U) = \begin{cases} U^2 - T_q U + q & \text{if } q \in Q, \\ U(U^2 - T_{q'} U + q') & \text{if } q = q'. \end{cases}$$

Let $A' = T(N_\varnothing)_{\mathcal{O}}[U_q, q \in Q \cup \{q'\}]/(P_q(U_q), q \in Q \cup \{q'\})$. Define a ring homomorphism $T(N_\varnothing Qq'^2)_{\mathcal{O}} \to A'$ as in Corollary 9.37 by letting the image of T_p be equal to T_p if $p \notin Q \cup \{q'\}$ and equal to U_p if $p = q \in Q \cup \{q'\}$. Define a ring homomorphism $A' \otimes_{T(N_\varnothing)_{\mathcal{O}}} T_\varnothing^{\flat} \to T_\varnothing^{\flat}$ by letting the image of U_p equal to $T_q^{\sharp}$ if $q \in Q$, and equal to 0 if $q = q'$. Then, the composition

$$T(N_\varnothing Qq'^2)_{\mathcal{O}} \longrightarrow A' \longrightarrow A' \otimes_{T(N_\varnothing)_{\mathcal{O}}} T_\varnothing^{\flat} \longrightarrow T_\varnothing^{\flat} \tag{10.25}$$

satisfies condition (10.23) □

DEFINITION 10.30. Define a maximal ideal $\mathfrak{m}_Q^{\natural}$ of $T(N_\varnothing, Qq'^2)_{\mathcal{O}} = T(N_\varnothing, Qq'^2)_{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathcal{O}$ to be the inverse image of the maximal ideal $\mathfrak{m}_\varnothing$ by the ring homomorphism $\tilde{t}_{\varnothing,Q} : T(N_\varnothing, Qq'^2)_{\mathcal{O}} \to T_\varnothing^{\flat}$. We call the completion $T(N_\varnothing, Qq'^2)_{\mathcal{O},\mathfrak{m}_Q^{\natural}}$ of $T(N_\varnothing, Qq'^2)_{\mathcal{O}}$ at the maximal ideal $\mathfrak{m}_Q^{\natural}$ the *full Hecke algebra*, and denote it by $T_Q^{\natural}$. The ring homomorphism induced by $\tilde{t}_{\varnothing,Q}$ is denoted by

$$t_{\varnothing,Q}^{\natural} : T_Q^{\natural} \longrightarrow T_\varnothing^{\flat}. \tag{10.26}$$

We can define an isomorphism $T_Q \to T_Q^{\natural}$; $T_p \mapsto \langle p \rangle^{-1/2} T_p$, $p \nmid N_\Sigma Q q' \ell$, but we do not use it in this book.

PROPOSITION 10.31. *$T_Q^{\natural}$ is reduced.*

PROOF. The proof is similar to that of Proposition 10.4. Define a subring $T'(N_\varnothing, Qq'^2)_{\mathcal{O}}$ of $T(N_\varnothing, Qq'^2)'_{\mathcal{O}}$ as the subring generated over $\mathcal{O}$ by T_p $(p \nmid N_\varnothing Qq'^2)$ and $\langle a \rangle$ $(a \in (\mathbf{Z}/Qq'^2\mathbf{Z})^\times)$. Let

$$\Phi(N_\varnothing, Qq'^2)_K = \operatorname{Spec} T'(N_\varnothing, Qq'^2)_K.$$

$T(N_\varnothing, Qq'^2)'_{\mathcal{O}}$ is reduced and $T(N_\varnothing, Qq'^2)'_K = \prod_{f \in \Phi(N_\varnothing, Qq'^2)_K} K_f$. Let $\mathfrak{m}'_Q$ be the maximal ideal of $T(N_\varnothing, Qq'^2)'_{\mathcal{O}}$ defined as the intersection $T(N_\varnothing, Qq'^2)'_{\mathcal{O}} \cap \mathfrak{m}^\natural_Q$. It suffices to show that the natural mapping $T(N_\varnothing, Qq'^2)'_{\mathcal{O},\mathfrak{m}'_Q} \to T^\natural_Q = T(N_\varnothing, Qq'^2)_{\mathcal{O},\mathfrak{m}^\natural_Q}$ becomes an isomorphism after tensoring $\otimes_{\mathcal{O}} K$.

Define a subset $\Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q} \subset \Phi(N_\varnothing, Qq'^2)_K$ by

$$\{f \in \Phi(N_\varnothing, Qq'^2)_K \,|\, \operatorname{Ker}(T(N_\varnothing, Qq'^2)'_{\mathcal{O}} \to K_f) \subset \mathfrak{m}'_Q\}.$$

Since we have $T(N_\varnothing, Qq'^2)'_{\mathcal{O},\mathfrak{m}'_Q} \otimes_{\mathcal{O}} K = \prod_{f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}} K_f$, it suffices to show that the natural mapping $K_f \to T^\natural_{Q,K} \otimes_{T(N_\varnothing, Qq'^2)'_K} K_f$ is an isomorphism for each primitive form $f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}$.

Let $f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}$. Since the level N_f of f satisfies $N_\varnothing | N_f | N_\varnothing Qq'^2$, if $p | N_\varnothing Qq'^2/N_f$, we have $p | Qq'$. As in the proof of Proposition 10.4, for a primitive form $f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}$ and a prime number $p | N_\varnothing Qq'^2/N_f$, define a polynomial $P_{f,p}(U) \in \mathcal{O}_f[U]$ in U by

$$P_{f,p}(U) = \begin{cases} U(U^2 - a_p(f)U + p) & \text{if } \operatorname{ord}_p N_\varnothing Qq'^2/N_f = 2, \\ U(U - a_p(f)) & \text{if } \operatorname{ord}_p N_\varnothing Qq'^2/N_f = 1 \text{ and } p | N_f, \\ U^2 - a_p(f)U + p & \text{if } \operatorname{ord}_p N_\varnothing Qq'^2/N_f = 1 \text{ and } p \nmid N_f, \end{cases}$$

and let $A_f = \mathcal{O}_f[U_p, p | N_\varnothing Qq'^2/N_f]/(P_{f,p}(U_p), p | N_\varnothing Qq'^2/N_f)$. There is an isomorphism $T(N_\varnothing, Qq'^2)_K \otimes_{T(N_\varnothing, Qq'^2)'_K} K_f \to A_f \otimes_{\mathcal{O}_f} K_f$ over K, and it induces a morphism of $\mathcal{O}$-algebras $T(N_\varnothing, Qq'^2)_{\mathcal{O}} \to A_f$. $T^\natural_{Q,K} \otimes_{T(N_\varnothing, Qq'^2)'_K} K_f$ can be identified with $(T^\natural_Q \otimes_{T(N_\varnothing, Qq'^2)_{\mathcal{O}}} A_f) \otimes_{\mathcal{O}} K$ through the isomorphism above. An ideal

$$\mathfrak{m}' = (U_q - \bar\alpha_q (q \in Q \text{ and } q | N_\varnothing Qq'^2/N_f), U_{q'} \ (q' | N_\varnothing Qq'^2/N_f))$$

of $A_{f,\mathbf{F}_f} = A_f \otimes_{\mathcal{O}_f} \mathbf{F}_f$ is a maximal ideal of $A_{f,\mathbf{F}_f}$, and it is a unique one whose inverse image in $T(N_\varnothing Qq'^2)_{\mathcal{O}}$ is $\mathfrak{m}^\natural_Q$. From this we see that $\mathcal{O}_f \to T^\natural_Q \otimes_{T(N_\varnothing, Qq'^2)_{\mathcal{O}}} A_f$ is an isomorphism, as in the proof of Proposition 10.4(2). □

By (10.24), the image of $\langle\ \rangle : (\mathbf{Z}/Qq'^2\mathbf{Z})^\times \to T_Q^{\natural\times}$ is contained in $1+\mathfrak{m}_Q^\natural$. Thus, the order M of this image is a power of ℓ. Since $\ell \neq 2$, M is odd. For $a \in (\mathbf{Z}/Qq'^2\mathbf{Z})^\times$, define $\langle a\rangle^{-1/2} = \langle a\rangle^{(M-1)/2}$. The character $\langle\ \rangle^{-1/2} : (\mathbf{Z}/Qq'^2\mathbf{Z})^\times \to 1+\mathfrak{m}_Q^\natural \subset T_Q^{\natural\times}$ satisfies $\langle\ \rangle\cdot(\langle\ \rangle^{-1/2})^2 = 1$. Let $\rho_Q : G_{\mathbf{Q}} \to \mathrm{GL}_2(R_Q)$ be the universal representation.

PROPOSITION 10.32. (1) *There exists a unique ring homomorphism*

$$f_Q^\natural : R_Q \longrightarrow T_Q^\natural \tag{10.27}$$

that satisfies

$$f_Q^\natural(\mathrm{Tr}(\rho_Q(\varphi_p))) = \langle p\rangle^{-1/2}T_p \tag{10.28}$$

for any prime number $p \nmid N_\varnothing Qq'\ell$.

(2) *The image of* $a \in (\mathbf{Z}/Q\mathbf{Z})^\times$ *by the mapping* $(\mathbf{Z}/Q\mathbf{Z})^\times \to \Delta_Q \to T_Q^{\natural\times}$ *induced by the composition* $\mathcal{O}[\Delta_Q] \to R_Q \to T_Q^\natural$ *is* $\langle a\rangle^{-1/2} \in T_Q^\natural$.

PROOF. (1) We define a ring homomorphism $f_Q^\natural : R_Q \to T_Q^\natural$. By the proof of Proposition 10.31, $T_Q^\natural\otimes_{\mathcal{O}}K \to \prod_{f\in\Phi(N_\varnothing,Qq'^2)_{K,\bar\rho,\bar\alpha_Q}} K_f$ is an isomorphism. We identify $T_Q^\natural \otimes_{\mathcal{O}} K$ with $\prod_{f\in\Phi(N_\varnothing,Qq'^2)_{K,\bar\rho,\bar\alpha_Q}} K_f$ through this isomorphism.

Let $\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ be the ℓ-adic representation associated with $f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}$. By Proposition 10.23(2), ρ_f is unramified at $p = q'$. Let $\varepsilon_f : (\mathbf{Z}/Qq'^2\mathbf{Z})^\times \to \mathcal{O}_f^\times$ be the character of f. ε_f is the composition of $\langle\ \rangle : (\mathbf{Z}/Qq'^2\mathbf{Z})^\times \to T_Q^{\natural\times}$ and $T_Q^{\natural\times} \to \mathcal{O}_f^\times$. Let δ_f be the composition of $\langle\ \rangle^{-1/2} : (\mathbf{Z}/Qq'^2\mathbf{Z})^\times \to T_Q^{\natural\times}$ and $T_Q^{\natural\times} \to \mathcal{O}_f^\times$. Then, we have $\varepsilon_f\delta_f^2 = 1$. Since ρ_f is unramified at q' and $\det\rho_f$ is the product of ε_f and the cyclotomic character, the conductors of ε_f and δ_f are divisors of Q. From now on, we regard ε_f and δ_f as characters of $(\mathbf{Z}/Q\mathbf{Z})^\times = \mathrm{Gal}(\mathbf{Q}(\zeta_Q)/\mathbf{Q})$. Regarding δ_f as a character $G_{\mathbf{Q}} \to \mathcal{O}_f^\times$, we define an ℓ-adic representation $\rho'_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ by $\rho'_f = \rho_f \otimes \delta_f$.

By Corollary 9.17, the ℓ-adic representation $\rho'_f = \rho_f\otimes\delta_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ is unramified at $p \nmid N_\varnothing Qq'\ell$, and we have $\det(1-\rho'_f(\varphi_p)t) = 1-\delta_f(p)a_p(f)t+\delta_f(p)^2\varepsilon_f(p)pt^2 = 1-\delta_f(p)a_p(f)t+pt^2$. Thus, $\rho'_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ is a lifting of $\bar\rho$, and $\det\rho'_f$ is the ℓ-adic cyclotomic character. Furthermore, by Theorem 9.31, ρ'_f is semistable at $p \in S_{\bar\rho} \cup \{\ell\}$, and if $\ell \notin S_{\bar\rho}$, ρ'_f is good at $p = \ell$. By Proposition 10.23(2), ρ'_f is unramified at $p = q'$. Thus, $\rho'_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ is a lifting of $\bar\rho$ of type $\mathcal{D}_Q$.

The lifting $\rho'_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ of $\bar\rho$ of type $\mathcal{D}_Q$ defines a ring homomorphism $R_Q \to \mathcal{O}_f$. For $p \nmid N_\varnothing Q q' \ell$, we have $\mathrm{Tr}(\rho'_f(\varphi_p)) = \varepsilon_f^{-1/2}(p) a_p(f)$. On the other hand, by Proposition 10.31, $T^\natural_Q \to \prod_{f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}} \mathcal{O}_f$ is injective, and the image of $\langle p \rangle^{-1/2} T_p$ is $(\varepsilon_f^{-1/2}(p) a_p(f))$. Thus, for $p \nmid N_\varnothing Q q' \ell$, the image of $\mathrm{Tr}(\rho_Q(\varphi_p))$ by the product $R_Q \to \prod_{f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}} \mathcal{O}_f$ coincides with the image of $\langle p \rangle^{-1/2} T_p$.

By Theorem 5.8, the subring $\mathcal{O}[\mathrm{Tr}(\rho_Q(\varphi_p)), p \nmid N_\varnothing Q q' \ell]$ of R_Q is dense. Thus, the image of the product $R_Q \to \prod_{f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}} \mathcal{O}_f$ is a subring of $T^\natural_Q$, and the ring homomorphism $f'_Q : R_Q \to T^\natural_Q$ has been constructed. The equation (10.28) has already been shown. The uniqueness is clear.

(2) Let $f \in \Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}$, and let $a \in (\mathbf{Z}/Q\mathbf{Z})^\times$. It suffices to show that the image of a by the composition $\mathcal{O}[(\mathbf{Z}/Q\mathbf{Z})^\times] \to R_Q \to T^\natural_Q \to K_f$ coincides with the image $\delta_f(a)$ of $\langle a \rangle^{-1/2}$ in K_f. Suppose $q \in Q$, and it suffices to show it in the case $a \in (\mathbf{Z}/q\mathbf{Z})^\times \subset \prod_{q \in Q} (\mathbf{Z}/q\mathbf{Z})^\times = (\mathbf{Z}/Q\mathbf{Z})^\times$. First, we show it in the case where the restriction $\varepsilon_{f,q} = \varepsilon_f|_{(\mathbf{Z}/q\mathbf{Z})^\times}$ is trivial. In this case, by Theorem 9.31(2), ρ_f is semistable at q. Thus, by Proposition 10.23(1), ρ_f is unramified at q. Hence, in this case, the images of $a \in (\mathbf{Z}/q\mathbf{Z})^\times$ in K_f both equal 1.

Suppose the restriction $\varepsilon_{f,q}$ is not trivial. Let χ be the ℓ-adic cyclotomic character. By Theorem 9.32, the restriction $\rho_f|_{G_{\mathbf{Q}_q}}$ is the direct sum of the unramified character $\alpha_q : G_{\mathbf{Q}_q} \to K_f^\times$ defined by $\alpha_q(\varphi_q) = a_q(f)$ and the ramified character $(\chi \cdot \varepsilon_f)|_{G_{\mathbf{Q}_q}} \cdot \alpha_q^{-1}$. By the definition of $\Phi(N_\varnothing, Qq'^2)_{K,\bar\rho,\bar\alpha_Q}$, we have $\alpha_q(\varphi_q) = a_q(f) \equiv \bar\alpha_q$. If $\delta_{f,q}$ is the q-component of δ_f, the product of characters $\alpha_q \cdot \delta_{f,q} : G^{\mathrm{ab}}_{\mathbf{Q}_q} \to \mathcal{O}_f^\times$ is a direct summand of the restriction $\rho'_{f,q}$, and we have $\alpha_q \cdot \delta_{f,q} \equiv \alpha_q$. Since the composition $R_Q \to T^\natural_Q \to \mathcal{O}_f$ is determined by $\rho'_{f,q}$, the q-component of the composition $(\mathbf{Z}/Q\mathbf{Z})^\times \to \Delta_Q \to T^{\natural\times}_Q \to \mathcal{O}_f^\times$ is $\delta_{f,q}$. This completes the proof in this case also. □

COROLLARY 10.33. *$t^{\natural}_{\varnothing,Q} : T^{\natural}_Q \to T^{\flat}_{\varnothing}$ induces an isomorphism of $\mathcal{O}$-algebras $T^{\natural}_{Q,K} \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} \to T_{\varnothing,K} = T^{\flat}_{\varnothing,K}$. The diagram*

$$\begin{tikzcd}
R_Q \arrow[r, "f^{\natural}_Q"] \arrow[d, "\tau_{\varnothing,Q}"'] & T^{\natural}_Q \arrow[d, "t^{\natural}_{\varnothing,Q}"] \\
R \arrow[r, "f"'] & T^{\flat}_{\varnothing}
\end{tikzcd}$$

is commutative.

PROOF. We identify as $T^{\natural}_{Q,K} = \prod_{f\in\Phi(N_{\varnothing},Qq'^2)_{K,\bar\rho,\bar\alpha_Q}} K_f, T_{\varnothing,K} = \prod_{f\in\Phi(N_{\varnothing})_{K,\bar\rho}} K_f$. By Theorem 9.31(1) and Proposition 10.32(2), we have $\Phi(N_{\varnothing})_{K,\bar\rho} = \{f \in \Phi(N_{\varnothing}, Qq'^2)_{K,\bar\rho,\bar\alpha_Q} \mid \rho_f$ is unramified at each $q \in Q\}$. By the proof of Proposition 10.32(2), that ρ_f is unramified at $q \in Q$ is equivalent to that the restriction $\varepsilon_{f,q}$ is trivial, which is in turn equivalent to that ρ'_f is unramified at $q \in Q$. By Corollary 10.24, this is still equivalent to that the composition $\mathcal{O}[\Delta_Q] \to K_f$ passes through the augmentation morphism $\mathcal{O}[\Delta_Q] \to \mathcal{O}$. This shows $T^{\natural}_{Q,K} \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} = \prod_{f\in\Phi(N_{\varnothing})_{K,\bar\rho}} K_f = T_{\varnothing,K}$. The commutativity of the diagram follows immediately from Theorem 5.8, and Propositions 10.29 and 10.32(1). ☐

DEFINITION 10.34. Consider the $T^{\natural}_Q$-module

$$M^{\natural}_Q = H_1(X_{0,1}(N_{\varnothing}, Qq'^2), \mathbf{Z})_{\mathcal{O}} \otimes_{T(N_{\varnothing},Qq'^2)_{\mathcal{O}}} T^{\natural}_Q$$

as an R_Q-module via the ring homomorphism (10.27) $f^{\natural}_Q : R_Q \to T^{\natural}_Q$. We also call this the *Hecke module*.

We show that the Hecke module $M^{\natural}_Q$ and the ring homomorphism (10.19) $\mathcal{O}[\Delta_Q] \to R_Q$ form a family of liftings of $(R, M) = (R_{\varnothing}, M_{\varnothing})$ along $\mathcal{O}[\Delta_Q]$. For a divisor d of Qq'^2, the composition of $X_{0,1}(N_{\varnothing}, Qq'^2) \to X_0(N_{\varnothing}Qq'^2)$ and $s_d : X_0(N_{\varnothing}Qq'^2) \to X_0(N_{\varnothing})$ is also denoted by $s_d : X_{0,1}(N_{\varnothing}, Qq'^2) \to X_0(N_{\varnothing})$. For $d|Qq'^2$, we define $a_d \in T^{\flat}_{\varnothing}$. For $q \in Q$, define $a_{0,q} = -T^{\sharp}_q, a_{1,q} = 1 \in T^{\flat}_{\varnothing}$, and define $a_{0,q'} = q', a_{1,q'} = -T_{q'}, a_{2,q'} = 1 \in T^{\flat}_{\varnothing}$. If $d = \prod_{q\in Q} q^{e_q} q'^{e_{q'}} | Qq'^2$, define $a_d = \prod_{q\in Q} a_{e_q,q} \cdot a_{e_{q'},q'} \in T^{\flat}_{\varnothing}$. The composition of $s_{d*} : H_1(X_{0,1}(N_{\varnothing}, Qq'^2), \mathbf{Z})_{\mathcal{O}} \to H_1(X_0(N_{\varnothing}), \mathbf{Z})_{\mathcal{O}}$ and $H_1(X_0(N_{\varnothing}), \mathbf{Z})_{\mathcal{O}} \to M_{\varnothing}$ is denoted by $\bar{s}_{d*}$. Similarly to Corollary 10.10, we can show the following.

PROPOSITION 10.35. *The $\mathcal{O}$-linear mapping*

$$\sum_{d|Qq'^2} a_d \bar{s}_{d*} : H_1(X_{0,1}(N_\varnothing, Qq'^2), \mathbf{Z})_\mathcal{O} \longrightarrow M_\varnothing \tag{10.29}$$

is compatible with the ring homomorphism $\tilde{t}_{\varnothing,Q} : T(N_\varnothing, Qq'^2) \to T^\flat_\varnothing$ in Proposition 10.29.

The proof is similar to that of Corollary 10.10, and we omit it.

The $\mathcal{O}$-linear mapping induced by homomorphism (10.29) is denoted by

$$m^\natural_{\varnothing,Q} : M^\natural_Q \longrightarrow M_\varnothing. \tag{10.30}$$

LEMMA 10.36. (1) *$T^\natural_Q$ and $M^\natural_Q$ are finitely generated free $\mathcal{O}$-modules.*

(2) *$M^\natural_{Q,K} = M^\natural_Q \otimes_\mathcal{O} K$ is free $T^\natural_{Q,K}$-module of rank* 2.

(3) *$m^\natural_{\varnothing,Q} : M^\natural_Q \to M_\varnothing$ is surjective.*

The proof of (1) is similar to that of Lemma 10.3, the proof of (2) is similar to that of Proposition 10.8, and the proof of (3) is similar to that of Proposition 10.11. Thus, we omit all these proofs.

PROPOSITION 10.37. *Let $Q \subset \mathcal{Q}$ be a finite subset. Through the homomorphism $\mathcal{O}[\Delta_Q] \to R_Q \to T^\natural_Q$, we consider $M^\natural_Q$ as an $\mathcal{O}[\Delta_Q]$-module. Then, $M^\natural_Q$ is a free $\mathcal{O}[\Delta_Q]$-module.*

This is Theorem 5.32(2) in Chapter 5. We will prove Proposition 10.37 in the next section.

PROPOSITION 10.38. *The RTM-triple $\mathcal{R}^\natural_Q = (R_Q, M^\natural_Q, \mathcal{O}[\Delta_Q] \to R_Q, r_{\varnothing,Q} : R_Q \to R_\varnothing, m_{\varnothing,Q} : M^\natural_Q \to M_\varnothing)$ is a lifting of $(R, M) = (R_\varnothing, M_\varnothing)$ along $(\mathcal{O}[\Delta_Q], \mathcal{O}[\Delta_Q] \to \mathcal{O})$.*

PROOF. We verify the conditions of Definition 5.24. R, R_Q are profinitely generated complete local $\mathcal{O}$-algebra, and the residue field of R is the same as that of $\mathcal{O}$. M is an R-module, and $M^\natural_Q$ is an R_Q-module. $\mathcal{O}[\Delta_Q]$ is a profinitely generated complete local $\mathcal{O}$-algebra, and $\mathcal{O}[\Delta_Q] \to \mathcal{O}$, $\mathcal{O}[\Delta_Q] \to R_Q$ and $r_{\varnothing,Q} : R_Q \to R$ are morphisms of local $\mathcal{O}$-algebras. By Lemma 10.25, the diagram

$$\begin{tikzcd}
\mathcal{O}[\Delta_Q] \arrow[r] \arrow[d] & R_Q \arrow[d, "r_{\varnothing,Q}"] \\
\mathcal{O} \arrow[r] & R
\end{tikzcd}$$

is commutative, and $R_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} \to R$ is an isomorphism. $m^\natural_{\varnothing,Q} : M^\natural_Q \to M = M_\varnothing$ is an $\mathcal{O}$-linear mapping compatible with $r_{\varnothing,Q} : R_Q \to R$ by Proposition 10.35 and Corollary 10.33.

We show $M^\natural_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} \to M$ is an isomorphism. By Proposition 10.37, the $\mathcal{O}$-linear mapping $M^\natural_Q$ is a free $\mathcal{O}[\Delta_Q]$-module. By Lemma 10.36(3), $M^\natural_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} \to M_\varnothing$ is a surjection of free $\mathcal{O}$-modules. Thus, it suffices to show $\operatorname{rank}_{\mathcal{O}} M^\natural_Q \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} = \operatorname{rank}_{\mathcal{O}} M_\varnothing$. Through the isomorphism $T^\natural_{Q,K} \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} \to T_{\varnothing,K}$ in Corollary 10.33, we consider $M^\natural_{Q,K} \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O}$ as a $T_{\varnothing,K}$-module. It suffices to show that both $M^\natural_{Q,K} \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O}$ and $M_{\varnothing,K}$ are free $T_{\varnothing,K}$-modules of rank 2. By Proposition 9.6 and Lemma 10.36(2), $M_{\varnothing,K}$ is a free $T_{\varnothing,K}$-module of rank 2, and $M^\natural_{Q,K}$ is a free $T^\natural_{Q,K}$-module of rank 2. By Corollary 10.33, we have $M^\natural_{Q,K} \otimes_{\mathcal{O}[\Delta_Q]} \mathcal{O} = M^\natural_{Q,K} \otimes_{T^\natural_{Q,K}} T_{\varnothing,K}$, and this is also a free $T_{\varnothing,K}$-module of rank 2. ☐

10.6. Proof of Proposition 10.37

We give a brief summary of perfect complex. Let A be a commutative ring.

DEFINITION 10.39. A complex of A-modules

$$C = (C_q, d_q : C_q \to C_{q-1})_{q \in \mathbf{Z}}$$

is said to be *right bounded* if there exists a such that $C_q = 0$ for $q \leq a$.

A complex of A-modules bounded below is called a *perfect complex* if there exist a complex $P = (P_q, d_q)_q$ of finitely generated projective A-modules such that $P_q = 0$ except for finitely many q and a morphism $f : P \to C$ of complexes of A-modules such that $f_* : H_q(P) \to H_q(C)$ are isomorphisms for all q.

In this section we assume A to be a commutative noetherian ring.

LEMMA 10.40. *Let C be a right-bounded complex of A-modules, and let $a \leq b$ be integers. The following are equivalent.*

(i) *There exist a complex $P = (P_q, d_q)_q$ of finitely generated projective A-modules such that $P_q = 0$ except for $a \leq q \leq b$ and a morphism $f : P \to C$ of complexes of A-modules such that $f_* : H_q(P) \to H_q(C)$ are isomorphisms for all q.*

(ii) *For any integer q, $H_q(C)$ is a finitely generated A-module, and except for $a \leq q \leq b$, $H_q(C) = 0$ and $\operatorname{Tor}_q^A(C, A/\mathfrak{m}) = 0$ for any maximal ideal $\mathfrak{m}$ of A.*

PROOF. (i) $\Rightarrow$ (ii) is clear. We show (ii) $\Rightarrow$ (i). Since A is noetherian, there exist a complex L of finitely generated free A-modules and a morphism of complexes of A-modules $f : L \to C$ such that $L_q = 0$ for $q < a$ and $f_* : H_q(L) \to H_q(C)$ are isomorphisms for all q. Let $P_b = \operatorname{Coker}(d_{b+1} : L_{b+1} \to L_b)$, and let P be the complex obtained by replacing L_b by P_b and L_q $(q > b)$ by 0. Then, for all q, $H_q(P) \to H_q(C)$ are isomorphisms. P_b is a finitely generated A-module, and for any maximal ideal $\mathfrak{m}$ of A, we have $\operatorname{Tor}_1^A(P_b, A/\mathfrak{m}) = \operatorname{Tor}_{b+1}^A(C, A/\mathfrak{m}) = 0$. Thus, P_b is a finitely generated projective A-modules, and $P \to C$ satisfies the condition. ☐

COROLLARY 10.41. *Let B be a commutative A-algebra, and let C be a right-bounded complex of B-modules. Let $\mathfrak{m}$ be a maximal ideal of A, let E be a flat B-module, and let q_1 be an integer. If $H_q(C) \otimes_B E$ is a finitely generated A-module for any integer q and for $q \neq q_1$, $H_q(C)_\mathfrak{m} = 0$, and $\operatorname{Tor}_q^A(C, A/\mathfrak{m}) = 0$, then $H_{q_1}(C)_\mathfrak{m} \otimes_B E$ is a finitely generated free $A_\mathfrak{m}$-module.*

PROOF. Since E is a flat B-module, we have $H_q(C \otimes_B E)_\mathfrak{m} = H_q(C)_\mathfrak{m} \otimes_B E$ and $\operatorname{Tor}_q^A(C \otimes_B E, A/\mathfrak{m}) \otimes_B E$ for any integer q. Thus, applying Lemma 10.40(ii) $\Rightarrow$ (i) to the complex of $A_\mathfrak{m}$-modules $A_\mathfrak{m} \otimes_A C \otimes_B E$ and $a = b = q_1$, we see that $H_{q_1}(C)_\mathfrak{m} \otimes_B E = P_{q_1}$ is a finitely generated projective $A_\mathfrak{m}$-module. Since $A_\mathfrak{m}$ is a local ring, this is a free module. ☐

For a locally constant sheaf $\mathcal{F}$ on a topological space X, the *singular chain complex* $C(X, \mathcal{F}) = (C_q(X, \mathcal{F}), d_q)$ is defined. For any integer $q \geq 0$, we have $C_q(X, \mathcal{F}) = \bigoplus_{f : \Delta^q \to X} \Gamma(\Delta^q, f^* \mathcal{F})$. Here, Δ^q is a standard q-simplex, and $f : \Delta^q \to X$ runs all continuous mappings. If $q < 0$, we define $C_q(X, \mathcal{F}) = 0$. $d_q : C_q(X, \mathcal{F}) \to C_{q-1}(X, \mathcal{F})$ is the alternating sum of the pullbacks by face mapping $\Delta^{q-1} \to \Delta^q$. For any integer q, we have $H_q(X, \mathcal{F}) = H_q(C(X, \mathcal{F}))$.

LEMMA 10.42. *Let G be a finite abelian group, let Y be a complex manifold, and let $\pi : X \to Y$ be a G-torsor. Let R be a commutative noetherian ring, and let $R[G]$ be the group algebra.*

(1) *With the action of $\sigma \in G$ defined as σ_*, the singular chain complex $C(X, R)$ is a complex of $R[G]$-modules. For an ideal I in*

$R[G]$, let $\overline{\mathcal{F}}$ be the sheaf $\pi_*R \otimes_{R[G]} R[G]/I$ on Y. $\overline{\mathcal{F}}$ is a locally constant sheaf, and $H_q(Y, \overline{\mathcal{F}}) = \mathrm{Tor}_q^{R[G]}(C(X,R), R[G]/I)$ for any integer q.

(2) *Furthermore, let $s_\lambda, t_\lambda : Y_\lambda \to Y, \lambda \in \Lambda$ be families of finite étale coverings, let $X_\lambda \to Y_\lambda, \lambda \in \Lambda$ be families of G-torsors, and let $s_\lambda, t_\lambda : X_\lambda \to X, \lambda \in \Lambda$ be finite étale coverings of G-torsors. For $\lambda, \mu \in \Lambda$, let $i_{\lambda,\mu} : X_{\lambda,\mu} = X_{\lambda}{}_{\searrow t_\lambda} \times_X {}_{s_\mu \swarrow} X_\mu \to X_{\mu,\lambda}$ be a homeomorphism that makes the diagram*

$$\begin{tikzcd}
X \arrow[d, equal] & X_{\lambda,\mu} \arrow[l, "s_\lambda \circ pr_1"'] \arrow[r, "t_\mu \circ pr_2"] \arrow[d, "i_{\lambda,\mu}"'] & X \arrow[d, equal] \\
X & X_{\mu,\lambda} \arrow[l, "s_\mu \circ pr_1"'] \arrow[r, "t_\lambda \circ pr_2"] & X
\end{tikzcd}$$

commutative.

Let T be the polynomial ring $R[G][T_\lambda, \lambda \in \Lambda]$. Then the singular chain complex $C(X,R)$ is a complex of T-modules, the multiplication by T_λ defined as $t_{\lambda *} \circ s_\lambda^*$ for $\lambda \in \Lambda$.

PROOF. (1) It is clear that $C(X,R)$ is a complex of $R[G]$-modules. We show it is a perfect complex.

Since $\pi : X \to Y$ is a G-torsor, π_*R is a locally constant sheaf of invertible $R[G]$-modules on Y. Thus, $\overline{\mathcal{F}}_I$ is a locally constant sheaf on Y. Since $C(Y, \overline{\mathcal{F}}_I) = C(Y, \pi_*R) \otimes_{R[G]} R[G]/I$ and $C(Y, \pi_*R) = C(X,R)$, we have $H_q(Y, \overline{\mathcal{F}}_I) = \mathrm{Tor}_q^{R[G]}(C(X,R), R[G]/I)$.

(2) For $\lambda, \mu \in \Lambda$, we have $T_\lambda \circ T_\mu = t_{\lambda *} \circ s_\lambda^* \circ t_{\mu *} \circ s_\mu^* = (t_\lambda \circ pr_2)_* \circ (s_\mu \circ pr_1)^*$. Similarly, we have $T_\mu \circ T_\lambda = (t_\mu \circ pr_2)_* \circ (s_\lambda \circ pr_1)^*$. Thus, by the assumption, we have $T_\lambda \circ T_\mu = T_\mu \circ T_\lambda$. Similarly, we have $\sigma_* \circ T_\lambda = T_\lambda \circ \sigma_*$, and thus $C(X,R)$ is a complex of T-modules. □

COROLLARY 10.43. *Let the notation be as in Lemma 10.42. Let E be a flat T-module, and let q_1 be an integer. Let $\mathfrak{m}$ be a maximal ideal of $R[G]$, and let $\overline{\mathcal{F}}_{\mathfrak{m}}$ be the locally constant sheaf $\pi_*R \otimes_{R[G]} R[G]/\mathfrak{m}$ on Y. Suppose $H_q(X,R) \otimes_T M$ is a finitely generated $R[G]$-module for any q and for any integer $q \neq q_1$, $H_q(X,R) \otimes_{R[G]} R[G]_{\mathfrak{m}} \otimes_T M = 0$ and $H_q(Y, \overline{\mathcal{F}}_{\mathfrak{m}}) \otimes_T M = 0$. Then, $H_{q_1}(X,R) \otimes_{R[G]} R[G]_m \otimes_T M$ is a finitely generated free $R[G]_{\mathfrak{m}}$-module.*

PROOF. Let $A = R[G]$, $B = T$, and $C = C(X,R)$. The singular chain complex $C(X,R)$ is a right-bounded complex of T-modules by Lemma 10.42. Since $\mathrm{Tor}_q^{R[G]}(C(X,R), R[G]/\mathfrak{m}) = H_q(Y, \overline{\mathcal{F}}_{\mathfrak{m}})$, it suffices to apply Corollary 10.41. □

LEMMA 10.44. *Let $N, M \geq 1$ be relatively prime integers, and let p be a prime number not dividing NM. The action of the Hecke operator $T_p = s_* \circ t^*$ on $H_0(Y_{0,1}(N,M), \mathbf{Z})$ is the multiplication by $p+1$.*

PROOF. It follows immediately from $\deg t = p+1$. □

PROPOSITION 10.45. *Let $N, M \geq 1$ be relatively prime integers, and let $r \geq 4$ be an integer relatively prime to NM. Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbf{Q}_\ell$, let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of $T_{0,1}(N, Mr)_{\mathcal{O}}$, and let $\mathfrak{m}_0$ be the inverse image of $\mathfrak{m}$ by $\mathcal{O}[(\mathbf{Z}/M\mathbf{Z})^\times] \to T_{0,1}(N, Mr)_{\mathcal{O}}$. Then, the localization $H_1(X_{0,1}(N, Mr), \mathbf{Z})_{\mathcal{O},\mathfrak{m}}$ is a finitely generated free $\mathcal{O}[(\mathbf{Z}/M\mathbf{Z})^\times]_{\mathfrak{m}_0}$-module.*

PROOF. Let $G = (\mathbf{Z}/M\mathbf{Z})^\times$ and $R = \mathcal{O}$, and let T be the polynomial ring $\mathcal{O}[G][T_p, p : \text{prime}]$ of infinite number of variables over $\mathcal{O}[G]$. Let $\overline{T}$ be the image of the ring homomorphism $T \to T_{0,1}(N, Mr)_{\mathcal{O}}$ that sends T_p to T_p, and let $\mathfrak{m}_T \subset T$, $\mathfrak{m}_{\overline{T}} \subset \overline{T}$ be the inverse images of $\mathfrak{m} \subset T_{0,1}(N, Mr)_{\mathcal{O}}$. Since $T_{0,1}(N, Mr)_{\mathcal{O}}$ and $\overline{T}$ are both complete semilocal rings, the localization $H_1(X_{0,1}(N, Mr), \mathbf{Z})_{\mathcal{O},\mathfrak{m}}$ is a direct summand of $H_1(X_{0,1}(N, Mr), \mathbf{Z})_{\mathcal{O},\mathfrak{m}_{\overline{T}}} = H_1(X_{0,1}(N, Mr), \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T}$. As in Lemma 10.20, the $\mathcal{O}[G]_{\mathfrak{m}_0}$-linear mapping

$$H_1(Y_{0,1}(N, Mr), \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T} \to H_1(X_{0,1}(N, Mr), \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T}$$

is an isomorphism. Thus, it suffices to show $H_1(Y_{0,1}(N, Mr), \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T}$ is a finitely generated free $\mathcal{O}[G]_{\mathfrak{m}_0}$-module.

Since we assume $r \geq 4$, $X = Y_{0,1}(N, Mr)$ and $Y = Y_{0,1}(NM, r)$ are fine moduli schemes, and $\pi : X \to Y$ is a G-torsor. Similarly to $s_n, t_n : I_0(N, n) \to X_0(N)$ in §9.1, we define finite étale coverings that induce Hecke operators. This family satisfies the condition of Lemma 10.42(2). We show $H_1(X, \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T} = H_1(X, \mathcal{O}) \otimes_{\mathcal{O}[G]} \mathcal{O}[G]_{\mathfrak{m}_0} \otimes_T T_{\mathfrak{m}_T}$ is a finitely generated free $\mathcal{O}[G]_{\mathfrak{m}_0}$ module by applying Corollary 10.43.

The localization $M = T_{\mathfrak{m}_T}$ is a flat T-module. Since $H_q(X, \mathbf{Z})_{\mathcal{O}}$ is a finitely generated $\mathcal{O}$-module, the image of T in $\mathrm{End}_{\mathcal{O}}(H_q(X, \mathbf{Z})_{\mathcal{O}})$ is finitely generated as $\mathcal{O}$-module, and the product of a finite number of complete local rings. Thus, $H_q(X, \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T}$ is a direct summand of $H_q(X, \mathbf{Z})_{\mathcal{O}}$, and a finitely generated $\mathcal{O}[G]$-module. Since X is an affine curve, we have $H_q(X, \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T} = 0$ and $H_q(Y, \overline{\mathcal{F}}_{\mathfrak{m}_0}) = 0$ for $q \neq 0, 1$. By Lemma 10.44, we have $H_0(X, \mathbf{Z})_{\mathcal{O},\mathfrak{m}_T} = 0$. Moreover, since the natural morphism $H_0(X, \mathcal{O}) = H_0(Y, \pi_* \mathcal{O}) \to H_0(Y, \overline{\mathcal{F}}_{\mathfrak{m}_0})$

is surjective, we have $H_0(Y, \overline{\mathcal{F}}_{\mathfrak{m}_0})_{\mathfrak{m}_T} = 0$. Thus, by Corollary 10.43, $H_1(X, \mathbf{Z})_{\mathcal{O}, \mathfrak{m}_T}$ is a finitely generated free $\mathcal{O}[G]_{\mathfrak{m}_0}$-module. ☐

PROOF OF PROPOSITION 10.37. We apply Proposition 10.45 to $N = N_\varnothing$, $M = Q$, and $r = q'^2$. Let $G = (\mathbf{Z}/Q\mathbf{Z})^\times$, and let $\mathfrak{m}_{\mathcal{O}[G]} \subset \mathcal{O}[G]$ be the inverse image of the maximal ideal $\mathfrak{m}_Q^\natural$ of $T_{0,1}(N, Mr)_\mathcal{O}$ by the ring homomorphism $\mathcal{O}[G] \to T_{0,1}(N, Mr)_\mathcal{O}$. Since the image of G by $\mathcal{O}[G] \to T_{0,1}(N, Mr)_\mathcal{O}/\mathfrak{m}_Q^\natural$ equals 1 and Δ_Q is the maximal ℓth power quotient of the finite abelian group G, the localization of $\mathcal{O}[G]$ at $\mathfrak{m}_{\mathcal{O}[G]}$ is $\mathcal{O}[\Delta_Q]$. Thus, by Proposition 10.45, $M_Q^\natural = H_1(X_{0,1}(N_\varnothing, Qq'^2), \mathbf{Z})_{\mathcal{O}, \mathfrak{m}_Q^\natural}$ is a finitely generated free $\mathcal{O}[\Delta_Q]$-module. ☐

10.7. Proof of Theorem 5.22

In this section, assuming Theorems 5.32(1) and 5.34, we will prove Theorem 5.22 along the idea explained in §5.6. Theorems 5.32(1) and 5.34 are related to Selmer groups, and will be proved in the next section. We prove the following stronger theorem.

THEOREM 10.46. *Let Σ be a finite set of primes such that $\Sigma \cap S_{\bar\rho} = \varnothing$. If $\ell \in \Sigma$, we assume $\bar\rho$ to be ordinary at ℓ. Then, $f_\Sigma : R_\Sigma \to T_\Sigma$ is an isomorphism, R_Σ is a complete intersection, M_Σ is a free T_Σ-module, and $i_\Sigma : T_\Sigma \to T_\Sigma^\flat$ is an isomorphism.*

PROOF. For the ring of integers $\mathcal{O}'$ of a finite extension K' of K, the natural mappings $R_{\Sigma,\mathcal{O}} \otimes_\mathcal{O} \mathcal{O}' \to R_{\Sigma,\mathcal{O}'}$ and $T_{\Sigma,\mathcal{O}} \otimes_\mathcal{O} \mathcal{O}' \to T_{\Sigma,\mathcal{O}'}$ are isomorphisms by Corollaries 5.10 and 5.19, and the natural mappings $M_{\Sigma,\mathcal{O}} \otimes_\mathcal{O} \mathcal{O}' \to M_{\Sigma,\mathcal{O}'}$ and $T^\flat_{\Sigma,\mathcal{O}} \otimes_\mathcal{O} \mathcal{O}' \to T^\flat_{\Sigma,\mathcal{O}'}$ are isomorphisms by definition. Thus, we may replace K by a finite extension.

By Proposition 5.14(2), $\Phi(N_\varnothing)_{K,\bar\rho}$ is nonempty. Thus, replacing K by its finite extension if necessary, we may assume there exists a primitive form $f \in \Phi(N_\varnothing)_{K,\bar\rho}(K)$ with K coefficients. Replacing further by an unramified quadratic extension if necessary, we may assume the eigenvalues of $\bar\rho(\varphi_p)$ are elements of $\mathbf{F}$ for each prime $p \nmid N_\Sigma \ell$.

Let $\pi_\varnothing : T_\varnothing \to \mathcal{O}$ be a ring homomorphism defined by a primitive form $f \in \Phi(N_\varnothing)_{K,\bar\rho}(K)$ with K coefficients, and let $\pi_\Sigma : T_\Sigma \to \mathcal{O}$ be the composition $\pi_\varnothing \circ t_{\varnothing,\Sigma}$. By Proposition 10.8, $\mathcal{R}_\Sigma = (R_\Sigma, T_\Sigma, M_\Sigma, f_\Sigma : R_\Sigma \to T_\Sigma, \pi_\Sigma : T_\Sigma \to \mathcal{O})$ is an *RTM*-triple of rank 2. By Proposition 5.29, if the *RTM*-triple $\mathcal{R}_\Sigma$ is complete, $i_\Sigma : T_\Sigma \to T_\Sigma^\flat$

is an isomorphism. Thus, we only have to show that the *RTM*-triple $\mathcal{R}_\Sigma$ is complete, in other words, Theorem 5.31.

We first show the *RTM*-triple $\mathcal{R}_\varnothing$ is complete. Let

$$r = \dim_{\mathbf{F}} \mathfrak{m}_{R_\varnothing}/(\mathfrak{m}_{\mathcal{O}} R_\varnothing + \mathfrak{m}^2_{R_\varnothing}).$$

By Proposition 10.26, there exists an odd prime $q' \in \widetilde{\mathcal{Q}}$ such that $q' \not\equiv 1 \bmod \ell$, and so choose such a q'. By Theorem 5.32(1), which will be proved in the next section, there exists for any positive integer n, a set $Q_n = \{q_1, \dots, q_r\}$ of r prime numbers such that

$$Q_n \subset \mathcal{Q},\ q_1, \dots, q_r \equiv 1 \bmod \ell^n,\ r = \dim_{\mathbf{F}} \mathfrak{m}_{R_{Q_n}}/(\mathfrak{m}_{\mathcal{O}} R_{Q_n} + \mathfrak{m}^2_{R_{Q_n}}).$$

Choose such Q_n for each n. By Proposition 10.38, the quintuple $\mathcal{R}^\natural_{Q_n} = (R_{Q_n}, M^\natural_{Q_n}, \mathcal{O}[\Delta_{Q_n}] \to R_{Q_n}, r_{\varnothing,Q_n} : R_{Q_n} \to R_\varnothing, m_{\varnothing,Q_n} : M^\natural_{Q_n} \to M_\varnothing)$ is a lifting of $(R, M) = (R_\varnothing, M_\varnothing)$ along $\mathcal{O}[\Delta_{Q_n}] \to \mathcal{O}$.

Let $\mathcal{O}_n$ be the group algebra $\mathcal{O}[(\mathbf{Z}/\ell^n\mathbf{Z})^r]$. For each n, take a surjection $\Delta_{Q_n} \to (\mathbf{Z}/\ell^n\mathbf{Z})^r$, and let $\mathcal{O}[\Delta_{Q_n}] \to \mathcal{O}_n$ be the induced ring homomorphism. Define a lifting $\mathcal{R}_n = (R_n, M_n, \mathcal{O}_n \to R_n, r_n : R_n \to R, m_n : M_n \to M)$ of (R, M) along the augmentation morphism $\mathcal{O}_n \to \mathcal{O}$ by $\mathcal{R}^\natural_{Q_n} \otimes_{\mathcal{O}[\Delta_{Q_n}]} \mathcal{O}_n = (R_{Q_n} \otimes_{\mathcal{O}[\Delta_{Q_n}]} \mathcal{O}_n, M^\natural_{Q_n} \otimes_{\mathcal{O}[\Delta_{Q_n}]} \mathcal{O}_n, \mathcal{O}_n \to R_{Q_n} \otimes_{\mathcal{O}[\Delta_{Q_n}]} \mathcal{O}_n, r_{\varnothing,Q_n} \otimes 1, m_{\varnothing,Q_n} \otimes 1)$.

By Proposition 10.37, $M^\natural_{Q_n}$ is a free $\mathcal{O}[\Delta_{Q_n}]$-module, and thus $M_n = M^\natural_{Q_n} \otimes_{\mathcal{O}[\Delta_{Q_n}]} \mathcal{O}_n$ is also a free $\mathcal{O}_n$-module. Applying Theorem 5.25, we conclude that R_Σ is a finitely generated $\mathcal{O}$-module, the ring $R_\varnothing$ is a complete intersection, and $M_\varnothing$ is a finitely generated free $R_\varnothing$-module. Thus, by Proposition 5.28, the *RTM*-triple $\mathcal{R}_\varnothing$ is complete. Moreover, by Proposition 10.4(2), the assumption of Proposition 5.29 is satisfied, and thus $i_\varnothing : T_\varnothing \to T^\flat_\varnothing$ is an isomorphism. This completes the proof of the case $\Sigma = \varnothing$.

We show the general case by induction on the number of elements of Σ. We have already shown the case $\Sigma = \varnothing$, and so we take $p \in \Sigma$ and let $\Sigma' = \Sigma - \{p\}$. We show $\mathcal{R}_\Sigma$ is complete assuming $\mathcal{R}_{\Sigma'}$ is complete. By Proposition 10.13, the quadruple $\mathcal{F}_{\Sigma',\Sigma} = (r_{\Sigma',\Sigma} : R_\Sigma \to R_{\Sigma'}, t_{\Sigma',\Sigma} : T_\Sigma \to T_{\Sigma'}, m_{\Sigma',\Sigma} : M_\Sigma \to M_{\Sigma'}, m^*_{\Sigma',\Sigma} : M_{\Sigma'} \to M_\Sigma)$ is a surjection $\mathcal{R}_\Sigma \to \mathcal{R}_{\Sigma'}$ of *RTM*-triples. By the assumption (hypothesis) of induction, $i_{\Sigma'} : T_{\Sigma'} \to T^\flat_{\Sigma'}$ is an isomorphism. Thus, even when $p = \ell$, $T_p \in T_{\Sigma'}$, and $\Delta_p \in T_{\Sigma'}$.

If $p = \ell$, let $T_p^\sharp \in T_{\Sigma'}$ be the root of $T^2 - T_pT + p = 0$ that is invertible, and define $\Delta_p \in T_{\Sigma'}$ by

$$\Delta_p = \begin{cases} (p-1)((p+1)^2 - T_p^2) & \text{if } p \neq \ell, \\ (T_p^{\sharp 2} - 1)(2T_p^\sharp - T_p) & \text{if } p = \ell. \end{cases}$$

By Proposition 10.14, Δ_p is the multiplier of the surjective morphism $\mathcal{F}_{\Sigma',\Sigma} : \mathcal{R}_\Sigma \to \mathcal{R}_{\Sigma'}$. If $p \neq \ell$, we have

$$\pi_{\Sigma'}(\Delta_p) = (p-1)((p+1)^2 - a_p(f)^2).$$

If $p = \ell$, then $2T_p^\sharp - T_p$, $p-1$ and $1 - p^2/T_p^{\sharp 2}$ are all invertible elements of $T_{\Sigma'}$, and thus we have

$$((p+1)^2 - T_p^2) = (1 + T_p + p)(1 - T_p + p) = (1 - T_p^{\sharp 2})(1 - p^2/T_p^{\sharp 2}).$$

Hence, in this case also, we have

$$\operatorname{ord}_{\mathcal{O}} \pi_{\Sigma'}(\Delta_p) = \operatorname{ord}_{\mathcal{O}}(p-1)((p+1)^2 - a_p(f)^2).$$

By Theorem 9.21, we have $(p+1)^2 - a_p(f)^2 \neq 0$ and

$$\begin{aligned} &\operatorname{length}_{\mathcal{O}} \operatorname{Ker}(\mathfrak{p}_{R_\Sigma}/\mathfrak{p}_{R_\Sigma}^2 \to \mathfrak{p}_{R_{\Sigma'}}/\mathfrak{p}_{R_{\Sigma'}}^2) \\ &\qquad \leq \operatorname{ord}_{\mathcal{O}}(p-1)((p+1)^2 - a_p(f)^2) = \operatorname{ord}_{\mathcal{O}} \pi_{\Sigma'}(\Delta_p). \end{aligned}$$

Thus, applying Theorem 5.27, the *RTM*-triple $\mathcal{R}_\Sigma$ is also complete. This completes the proof of Theorem 5.31, and thus Theorems 10.46 and 5.22. ☐

CHAPTER 11

Selmer groups

In this chapter we study Selmer groups and describe the relation between the Selmer groups and the deformation rings. Then, by studying the order of Selmer groups, we prove Theorems 5.32(1) and 5.34, which completes the proof of Theorem 5.22. In §11.1 and §11.2, we will introduce cohomology of groups and Galois cohomology and show their fundamental properties.

In §11.3, we will introduce Selmer groups and describe its relation with deformation rings. We translate Theorems 5.32(1) and 5.34 into the properties of Selmer groups in Theorem 11.37 and Proposition 11.38. In §11.5, we will calculate the order of local cohomology groups and prove Proposition 11.38. In §11.6, we will prove Theorem 11.37 using group theoretic properties of subgroups of $\mathrm{GL}_2(\mathbf{F})$.

11.1. Cohomology of groups

Definition 11.1. (1) The projective limit $G = \varprojlim_{\lambda\in\Lambda} G_\lambda$ of a projective system $(G_\lambda)_{\lambda\in\Lambda}$ of surjections of finite groups is called a *profinite group*.

(2) Let G be a profinite group, and let R be a commutative ring. A finite R-module M is called a *finite R-G-module* if a continuous homomorphism $G \to \mathrm{Aut}_R(M)$ of a finite discrete group $\mathrm{Aut}_R(M)$ is given. If $R = \mathbf{Z}$, a finite $\mathbf{Z}$-G-module is simply called a *finite G-module*.

If F is a field, its absolute Galois group G_F is a profinite group. For a profinite group G and a finite R-G-module M, the cohomology group $H^q(G, M), q = 0, 1, 2, \ldots$, is defined as R-modules. The cases where $q = 0, 1$ are particularly important, and we first give a definition in these cases.

Definition 11.2. Let G be a profinite group, let R be a commutative ring, and let M be a finite R-G-module.

(1) $H^0(G,M)$ is defined as the G-invariant part of M

$$M^G = \{x \in M \mid gx = x \text{ for any } g \in G\}.$$

(2) A continuous mapping $c : G \to M$ is called a 1-*cocycle* if it satisfies $c(gh) = c(g) + gc(h)$ for any $g, h \in G$. For $x \in M$, let $c_x : G \to M$ be the 1-cocycle defined by $c_x(g) = gx - x$. Let $Z^1(G,M)$ be the R-module of all 1-cocycles, and define

$$H^1(G,M) = Z^1(G,M)/\{c_x \mid x \in M\}.$$

$H^0(G, M)$ and $H^1(G, M)$ naturally have a structure of R-module.

LEMMA 11.3. *Let G be a finite group of order n, and let R be a commutative ring. For any R-G-module M, we have $n \cdot H^1(G, M) = 0$. In particular, if n is invertible in R, we have $H^1(G, M) = 0$.*

PROOF. Let $c \in Z^1(G, M)$ be a 1-cocycle, and let $b = \sum_{h\in G} c(h)$. Since $b - gb = \sum_{h\in G}(c(gh) - gc(h)) = nc(g)$, we have $n[c] = 0 \in H^1(G, M)$. ☐

For a finite G-module M, the G-*coinvariant quotient* is defined by $M/(gx - x : g \in G, x \in M)$ and is denoted by M_G.

LEMMA 11.4. *Let G be a profinite group, let R be a commutative ring, and let M be a finite R-G-module.*

(1) *If the action of G on M is trivial, $H^1(G, M)$ equals the R-module* $\mathrm{Hom}(G, M)$ *of all continuous homomorphisms $G \to M$.*

(2) *Let $G = \widehat{\mathbf{Z}} = \varprojlim_n \mathbf{Z}/n\mathbf{Z}$ be the profinite completion of $\mathbf{Z}$. Then, the mapping that sends the class of a 1-cocycle $c : G \to M$ to the class of $c(1)$*

$$H^1(G,M) \longrightarrow M_G \tag{11.1}$$

is an isomorphism.

PROOF. (1) Clear from Definition 11.2.

(2) The mapping $Z^1(G,M) \to M : c \mapsto c(1)$ is a bijection. This induces the isomorphism (11.1). ☐

If G is a profinite group, a homomorphism of finite R-G-modules $M \to N$ induces an R-linear mapping $H^q(G,M) \to H^q(G,N)$. Also, if $G \to H$ is a continuous homomorphism of profinite groups and M is a finite R-H-module, then an R-linear mapping $H^q(H,M) \to H^q(G,M)$ is defined by regarding M as an R-G-module through

$G \to H$. If a homomorphism $G \to H$ is injective, the induced homomorphism $H^q(H, M) \to H^q(G, M)$ is called the restriction mapping. If $(N_\lambda)_{\lambda \in \Lambda}$ is a fundamental neighborhood system of the identity element consisting of open normal subgroups of G, the morphism $H^1(G, M) \to \varinjlim_\lambda H^1(G/N_\lambda, M^{N_\lambda})$ is an isomorphism.

PROPOSITION 11.5. *Let G be a profinite group, and let N be its closed normal subgroup. If M is a finite G-module, the natural mappings form an exact sequence*

$$0 \longrightarrow H^1(G/N, M^N) \longrightarrow H^1(G, M) \longrightarrow H^1(N, M)^G.$$

PROOF. It is easy to see that the image of the restriction mapping $H^1(G, M) \to H^1(N, M)$ is contained in the G-invariant part $H^1(N, M)^G$. Also, the composition $H^1(G/N, M^N) \to H^1(G, M) \to H^1(N, M)^G$ is the 0 mapping.

We show $H^1(G/N, M^N) \to \operatorname{Ker}(H^1(G, M) \to H^1(N, M)^G)$ is surjective. Let $c : G \to M$ be a 1-cocycle. Assuming the class $[c]$ belongs to $\operatorname{Ker}(H^1(G, M) \to H^1(N, M)^G)$, we show $[c]$ is in the image of $H^1(G/N, M^N) \to H^1(G, M)$. There exists an $x \in M$ such that $c(h) = hx - x$ for any $h \in N$. Replacing c by the 1-cocycle $c' : G \to M$ defined by $c'(g) = c(g) - (g(x) - x)$, we may assume $c|_N = 0$. Then, for any $g \in G$ and $h \in N$, we have $c(gh) = c(g) + gc(h) = c(g), hc(g) = c(hg) - c(h) = c(g \cdot g^{-1}hg) = c(g)$, and thus $c : G \to M$ induces $\bar{c} : G/N \to M^N$. Since the class $[c] \in H^1(G, M)$ is the image of $[\bar{c}] \in H^1(G/N, M^N)$, we conclude that $H^1(G/N, M^N) \to \operatorname{Ker}(H^1(G, M) \to H^1(N, M)^G)$ is surjective.

We show $H^1(G/N, M^N) \to H^1(G, M)$ is injective. Let $c : G/N \to M^N$ be a 1-cocycle. Suppose the image of $[c] \in H^1(G/N, M^N)$ in $H^1(G, M)$ is 0. Then, there exists an $x \in M$ such that $c(\bar{g}) = gx - x$ for any $g \in G$. Since $hx = x + c(\bar{h}) = x$ for any $h \in N$, we see $x \in M^N$. This proves $[c] = 0$. □

COROLLARY 11.6. *Let p be a prime number. Let G be a profinite group, and let $N \subset G$ be a closed normal subgroup. Suppose N is the projective limit of a projective system of finite groups of order relatively prime to p, and suppose G/N is isomorphic to $\mathbf{Z}_p$. If M is a finite $\mathbf{Z}_p$-G-module, then there is a natural isomorphism*

$$H^1(G, M) \longrightarrow \operatorname{Hom}(G/N, M_N).$$

PROOF. By Lemma 11.3, we have $H^1(N, M) = 0$. Thus, we obtain an isomorphism $H^1(G/N, M^N) \to H^1(G, M)$, by Proposition 11.5. The invariant part M^N is naturally identified with coinvariant quotient M_N. The rest of the proof goes similarly with Lemma 11.4(2). ☐

For a commutative ring, define $R[\varepsilon] = R[X]/(X^2)$. ϵ represents the image of X. $R[\varepsilon] = R + R\epsilon$ is a free R-module of rank 2 with $\varepsilon^2 = 0$. For an R-module M, define an $R[\epsilon]$-module $\widetilde{M}$ by $R[\varepsilon] \otimes_R M = M + \varepsilon M$. We have a natural isomorphism $\widetilde{M}/\varepsilon M \to M$.

DEFINITION 11.7. Let G be a profinite group, let R be a commutative ring, and let M be a finite R-G-module.

(1) For a continuous homomorphism $\tilde{\rho} : G \to \mathrm{Aut}_{R[\varepsilon]}(\widetilde{M})$, consider $\widetilde{M}$ as a finite $R[\varepsilon]$-G-module through $\tilde{\rho}$, and denote it by $\widetilde{M}_{\tilde{\rho}}$. We call $\widetilde{M}_{\tilde{\rho}}$ an *infinitesimal lifting* if the natural homomorphism $\tilde{M}_{\tilde{\rho}}/\varepsilon M \to M$ of R-modules is an isomorphism of R-G-modules. The set of all infinitesimal liftings of M is denoted by $\mathrm{Lift}_{R\text{-}G}(M)$.

(2) An isomorphism of infinitesimal liftings $\widetilde{M}_{\tilde{\rho}}$ and $\widetilde{M}_{\tilde{\rho}'}$ is an isomorphism of $R[\varepsilon]$-G-modules $\widetilde{M}_{\tilde{\rho}} \to \widetilde{M}_{\tilde{\rho}'}$ such that the induced map $M \to M$ on the quotients is the identity. An isomorphism class of infinitesimal liftings of M is called an *infinitesimal deformation* of M, and is denoted by $\mathrm{Def}_{R\text{-}G}(M)$.

(3) Let M be a finitely generated free R-module, and let $\widetilde{M}_{\tilde{\rho}}$ be an infinitesimal lifting. We say $\widetilde{M}_{\tilde{\rho}}$ *preserves the determinant* if $\det \tilde{\rho} : G \to R[\varepsilon]^\times$ and $\det \rho : G \to R^\times \subset R[\varepsilon]^\times$ are equal. The set of all infinitesimal liftings that preserve the determinant is denoted by $\mathrm{Lift}^0_{R\text{-}G}$, and the set of all infinitesimal deformations that preserve the determinant is denoted by $\mathrm{Def}^0_{R\text{-}G}$.

Let G be a profinite group, let R be a commutative ring, and let M be a finite R-G-module. Define an action of G on $\mathrm{End}_R(M)$ by $g(f) = g \circ f \circ g^{-1}$ for $f \in \mathrm{End}_R(M), g \in G$. $\mathrm{End}_R(M)$ becomes a finite R-G-module. For $f \in \mathrm{End}_R(M)$, define an automorphism $1+\varepsilon f$ of $\widetilde{M}$ by $(1+\varepsilon f)(x+\varepsilon y) = x+\varepsilon(f(x)+y)$. Define a homomorphism of groups $\mathrm{End}_R(M) \to \mathrm{Aut}_{R[\varepsilon]}(\widetilde{M})$ by associating $1+\varepsilon f$ to $f \in \mathrm{End}_R(M)$, and we obtain an isomorphism of groups

$$\mathrm{End}_R(M) \to \mathrm{Ker}(\mathrm{Aut}_{R[\varepsilon]}(\tilde{M}) \to \mathrm{Aut}_R(M)).$$

For a 1-cocycle $c : G \to \mathrm{End}_R(M)$, define an action $\tilde{\rho}_c$ of G on $\widetilde{M}$ by $(1+\varepsilon c(g)) \circ (1 \otimes g)$. Then, $\widetilde{M}$ is an infinitesimal lifting of M. Thus, we obtain a natural mapping

$$Z^1(G, \mathrm{End}_R(M)) \longrightarrow \mathrm{Lift}_{R\text{-}G}(M). \tag{11.2}$$

PROPOSITION 11.8. *Let G be a profinite group, let R be a commutative ring, and let M be a finite R-G-module.*

(1) *The natural mapping* (11.2) *is bijective, and it induces a bijection*

$$H^1(G, \mathrm{End}_R(M)) \longrightarrow \mathrm{Def}_{R\text{-}G}(M). \tag{11.3}$$

(2) *Suppose M is finitely generated and free as an R-module, and let* $\mathrm{End}^0_R(M)$ *be the kernel of* $\mathrm{Tr} : \mathrm{End}_R(M) \to R$. *Then, the mapping* $Z^1(G, \mathrm{End}^0_R(M)) \to \mathrm{Lift}^0_{R\text{-}G}(M)$ *induced by the bijection* (11.2) *is also a bijection. Furthermore, if the rank of M is invertible in R, it induces a bijection*

$$H^1(G, \mathrm{End}^0_R(M)) \longrightarrow \mathrm{Def}^0_{R\text{-}G}(M). \tag{11.4}$$

PROOF. (1) Clear from the definition.

(2) The determinant of the action $\tilde{\rho}_c(g)$ is $\det g \cdot (1+\varepsilon \cdot \mathrm{Tr}\ c(g))$. Thus, the bijection $Z^1(G, \mathrm{End}_R(M)) \to \mathrm{Lift}_{R\text{-}G}(M)$ induces the bijection $Z^1(G, \mathrm{End}^0_R(M)) \to \mathrm{Lift}^0_{R\text{-}G}(M)$. We show the mapping (11.4) is bijective if the rank r of M is invertible in R. By definition, $\mathrm{Def}^0_{R\text{-}G}(M)$ is the image of $\mathrm{Lift}^0_{R\text{-}G}(M) \to \mathrm{Def}_{R\text{-}G}(M)$. Thus, it suffices to show that $H^1(G, \mathrm{End}^0_R(M)) \to H^1(G, \mathrm{End}_R(M))$ is injective. If the rank r is invertible in R, we have $\mathrm{End}_R(M) = \mathrm{End}^0_R(M) \oplus R$, from which the assertion follows immediately. ☐

Let G be a profinite group, let R be a commutative ring, and let M, N be finite R-G-modules. A finite R-G-module E together with an exact sequence of finite R-G-modules $0 \to N \to E \to M \to 0$ is called an *extension* of M by N. Two extensions E and E' of M by N are said to be isomorphic if there exists a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & N \arrow[r] & E' \arrow[r] & M \arrow[r] & 0.
\end{tikzcd}$$

For extensions E and E', the sum is defined to be

$$\mathrm{Ker}(E \oplus E' \xrightarrow{-} M) / \mathrm{Im}(N \xrightarrow{+} E \oplus E').$$

Here, $- : E \oplus E' \to M$ is the difference between $E \to M$ and $E' \to M$, and $+ : N \to E \oplus E'$ is the sum of $N \to E$ and $N \to E'$. For an extension E and $a \in R$, define the multiplication by a to be $\operatorname{Coker}((1, -a) : N \to E \oplus N)$. The set of isomorphism classes of extensions of M by N, denoted by $\operatorname{Ext}_{R\text{-}G}(M, N)$, has a structure of an R-module by this operation. If $G = 1$, we write $\operatorname{Ext}_{R\text{-}G}(M, N)$ simply by $\operatorname{Ext}_R(M, N)$.

An infinitesimal deformation $\widetilde{M}$ of M defines an extension of M by M. This defines a natural injection $\operatorname{Def}_{R\text{-}G}(M) \to \operatorname{Ext}_{R\text{-}G}(M, M)$, and its image equals the kernel of the mapping $\operatorname{Ext}_{R\text{-}G}(M, M) \to \operatorname{Ext}_R(M, M)$. Through this injection, we consider $\operatorname{Def}_{R\text{-}G}(M)$ as a submodule of $\operatorname{Ext}_{R\text{-}G}(M, M)$.

PROPOSITION 11.9. *Let G be a profinite group, and let R be a commutative ring. For R-G-modules M and N, we have a natural injection*

$$H^1(G, \operatorname{Hom}_R(M, N)) \longrightarrow \operatorname{Ext}_{R\text{-}G}(M, N). \tag{11.5}$$

The image of (11.5) *is the kernel of* $\operatorname{Ext}_{R\text{-}G}(M, N) \to \operatorname{Ext}_R(M, N)$.

If $M = N$, the image of (11.5) *is* $\operatorname{Def}_{R\text{-}G}(M) \subset \operatorname{Ext}_{R\text{-}G}(M, N)$, *and the natural morphism* (11.5) *coincides with* (11.3). *If M is a projective R-module, the morphism* (11.5) *is an isomorphism. In particular, if $M = R$, $H^1(G, N) \to \operatorname{Ext}_{R\text{-}G}(R, N)$ is an isomorphism.*

PROOF. If we define an action of G on $M \oplus N$ by $g(x, y) = (gx, c(g)gx + gy)$ for 1-cocycle $c : G \to \operatorname{Hom}_R(M, N)$, then $M \oplus N$ becomes an R-G-module. We denote by E_c this extension of M by N. Sending a 1-cocycle $c : G \to \operatorname{Hom}_R(M, N)$ to the class of the extension E_c, we obtain an R-linear mapping $Z^1(G, \operatorname{Hom}_R(M, N)) \to \operatorname{Ext}_{R\text{-}G}(M, N)$.

It is easy to see that the extensions E_c and E_0 are isomorphic if and only if there exists an R-linear mapping $f : M \to N$ satisfying $c(g) = gfg^{-1} - f$. Thus, we obtain a natural injection $H^1(G, \operatorname{Hom}_R(M, N)) \to \operatorname{Ext}_{R\text{-}G}(M, N)$. By the definition of (11.5), it is clear that the image coincides with the kernel of $\operatorname{Ext}_{R\text{-}G}(M, N) \to \operatorname{Ext}_R(M, N)$.

It is clear from the definition that (11.5) and (11.3) coincide if $M = N$. If M is a projective R-module, we have $\operatorname{Ext}_R(M, N) = 0$, and thus (11.5) is an isomorphism. □

For a general integer $q \geq 0$, the cohomology of group $H^q(G, M)$ is defined as follows. Let G be a profinite group, let R be a commutative ring, and let M be a finite R-G-module. For an integer $q \geq 0$, define $C^q(G, M) = \{\text{continuous mapping } G^q \to M\}$. For $f \in C^q(G, M)$, define $d^q f \in C^{q+1}(G, M)$ by

$$\begin{aligned} d^q f(g_0, \ldots, g_q) = g_0 f(g_1, \ldots, g_q) & \\ & - f(g_0 g_1, g_2, \ldots, g_q) + f(g_0, g_1 g_2, \ldots, g_q) \\ & - \cdots + (-1)^q f(g_0, \ldots, g_{q-2}, g_{q-1} g_q) \\ & \qquad + (-1)^{q+1} f(g_0, \ldots, g_{q-2}, g_{q-1}). \end{aligned}$$

For $q = -1$, define $C^{-1}(G, M) = 0$ and $d^{-1} = 0$. For $q \geq 0$, define

$$H^q(G, M) = \frac{\operatorname{Ker}(d^q : C^q(G, M) \to C^{q+1}(G, M))}{\operatorname{Im}(d^{q-1} : C^{q-1}(G, M) \to C^q(G, M))}.$$

This definition coincides with Definition 11.2 for $q = 0, 1$. For an exact sequence of finite R-G-modules $0 \to M' \to M \to M'' \to 0$, we have a long exact sequence

$$\begin{aligned} 0 \longrightarrow H^0(G, M') \longrightarrow H^0(G, M) \longrightarrow H^0(G, M'') & \\ \longrightarrow H^1(G, M') \longrightarrow H^1(G, M) \longrightarrow H^1(G, M'') & \\ \longrightarrow H^2(G, M') \longrightarrow H^2(G, M) \longrightarrow H^2(G, M'') & \longrightarrow \cdots. \end{aligned}$$

Let M, N, L be finite R-G-modules. An R-bilinear mapping $M \times N \to L$ is a bilinear mapping of finite R-G-modules if $(gx, gy) = g(x, y)$ for any $x \in M, y \in N, g \in G$. A bilinear mapping of R-G-modules $M \times N \to L$ induces a bilinear mapping of R-modules $\cup : H^p(G, M) \times H^q(G, N) \to H^{p+q}(G, L)$. This is called the *cup product*.

Let ℓ be a prime number, and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbf{Q}_\ell$. Let R be a profinitely generated complete local $\mathcal{O}$-algebra, and let $\mathfrak{m}$ be its maximal ideal. A finitely generated R-module M is a G-module if a continuous homomorphism $G \to \operatorname{Aut}_R(M) = \varprojlim_n \operatorname{Aut}_{R/\mathfrak{m}^n}(M/\mathfrak{m}^n M)$ is given. For an integer $q \geq 0$, define

$$H^q(G, M) = \varprojlim_n H^q(G, M/\mathfrak{m}^n M).$$

$H^q(G, M)$ is an R-module.

11.2. Galois cohomology

The group cohomology of the absolute Galois group G_F of a field is called Galois cohomology. In this section we present fundamental properties of Galois cohomology of p-adic fields and the rational number fields, Propositions 11.18, 11.20, 11.25, and 11.27. We do not give proofs to them, but instead we give typical examples in Examples 11.15, 11.19, 11.21, and 11.26.

DEFINITION 11.10. Let F be a field, and let $G_F = \mathrm{Gal}(\overline{F}/F)$ be the absolute Galois group of F. For a finite G_F-module M, define

$$H^q(F, M) = H^q(G_F, M).$$

For an integer $n \geq 1$, we consider $\mathbf{Z}/n\mathbf{Z}$ as a trivial G_F-module. By Lemma 11.4(1), we have

$$H^1(F, \mathbf{Z}/n\mathbf{Z}) = \mathrm{Hom}(G_F^{\mathrm{ab}}, \mathbf{Z}/n\mathbf{Z}). \tag{11.6}$$

Let $n \geq 0$ be an integer invertible in F. Let μ_n be the finite G_F-module of nth roots of unity $\{x \in \bar{F}^\times | x^n = 1\}$. For a finite $\mathbf{Z}/n\mathbf{Z}$-G_F-module M, let $M^\vee$ be the dual module $\mathrm{Hom}(M, \mathbf{Z}/n\mathbf{Z})$, and $M(1)$ the *Tate twist* $M \otimes \mu_n$.

PROPOSITION 11.11. *Let F be a field, and let $n \geq 1$ be an integer invertible in F.*

(1) *There is a natural isomorphism*

$$F^\times/(F^\times)^n \longrightarrow H^1(F, \mu_n). \tag{11.7}$$

(2) *Let* $\mathrm{Br}(F)$ *be the* Brauer group *of F* (§8.2(c) in *Number Theory 2*). *Let ${}_n\mathrm{Br}(F) = \{x \in \mathrm{Br}(F) \mid nx = 0\}$ be its n-torsion subgroup. Then, we have a natural isomorphism*

$$ {}_n\mathrm{Br}(F) \longrightarrow H^2(F, \mu_n). \tag{11.8}$$

We do not give a proof in this book. The natural isomorphism $F^\times/(F^\times)^n \to H^1(F, \mu_n)$ is defined as follows. For $a \in F^\times$, take its nth root $\alpha \in \overline{F}$, and let $c_a : G_F \to \mu_n$ be the 1-cocycle defined by $c_a(\sigma) = \sigma(\alpha)/\alpha$. The natural isomorphism is defined by sending a to the class of c_a.

Let E be an elliptic curve over F, and let $n \geq 1$ be an integer invertible in F. Let $E[n]$ be the finite G_F-module of n-torsion points of E. Similarly to the natural isomorphism $F^\times/(F^\times)^n \to H^1(F, \mu_n)$, we define a natural injection $E(F)/nE(F) \to H^1(F, E[n])$ as follows. For $a \in E(F)$, take $\alpha \in E(\bar{F})$ satisfying $a = n\alpha$, and let $c_a : G_F \to E[n]$ be the 1-cocycle defined by $c_a(\sigma) = \sigma(\alpha) - \alpha$. The natural injection is defined by sending a to the class of c_a.

Let F be a finite field $\mathbf{F}_p$. We have an isomorphism $\widehat{\mathbf{Z}} \to G_{\mathbf{F}_p}$ from the profinite completion of $\mathbf{Z}$ by sending 1 to the Frobenius substitution $\varphi_p \in G_{\mathbf{F}_p}$. Thus, by Lemma 11.4(2), we obtain a natural isomorphism $H^1(\mathbf{F}_p, M) \to M_{G_{\mathbf{F}_p}} : c \mapsto c(\varphi_p)$ for a finite $G_{\mathbf{F}_p}$-module M.

LEMMA 11.12. *Let p be a prime number.*

(1) *Let M be a finite $G_{\mathbf{F}_p}$-module. Then, $H^0(\mathbf{F}_p, M)$ and $H^1(\mathbf{F}_p, M)$ are finite groups, and the order of $H^0(\mathbf{F}_p, M)$ is the same as that of $H^1(\mathbf{F}_p, M)$.*

(2) *Let ℓ be a prime number, and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbf{Q}_\ell$. Let M be a finitely generated free $\mathcal{O}$-module with a continuous action of $G_{\mathbf{F}_p}$. If the action of the Frobenius substitution φ_p does not have an eigenvalue 1, the $\mathcal{O}$-module $H^1(\mathbf{F}_p, M)$ is finite and we have*

$$\operatorname{length}_{\mathcal{O}} H^1(\mathbf{F}_p, M) = \operatorname{ord}_{\mathcal{O}} \det(1 - \varphi_p : M).$$

PROOF. (1) Clear from the exact sequence

$$0 \longrightarrow M^{G_{\mathbf{F}_p}} \longrightarrow M \xrightarrow{1-\varphi_p} M \longrightarrow M_{G_{\mathbf{F}_p}} \longrightarrow 0.$$

(2) By Lemma 11.4(2), we obtain an isomorphism $H^1(\mathbf{F}_p, M) \to M_{G_{\mathbf{F}_p}} \to \operatorname{Coker}(1 - \varphi_p : M \to M)$. Thus, the assertion is clear by elementary linear algebra on $\mathcal{O}$-modules. ☐

Next, we consider the case where F is the p-adic field $\mathbf{Q}_p$. We identify naturally the quotient of the absolute Galois group $G_{\mathbf{Q}_p}$ by the inertia group I_p with the absolute Galois group $G_{\mathbf{F}_p}$ of the residue field. If the order of a finite $G_{\mathbf{Q}_p}$-module M is relatively prime to p, the kernel $\operatorname{Ker}(H^1(\mathbf{Q}_p, M) \to H^1(I_p, M))$ of the restriction mapping is called the *unramified part* of $H^1(\mathbf{Q}_p, M)$, and is denoted by $H^1_f(\mathbf{Q}_p, M)$. By Proposition 11.5, the unramified part $H^1_f(\mathbf{Q}_p, M)$ is the image of the injection $H^1(\mathbf{F}_p, M^{I_p}) \to H^1(\mathbf{Q}_p, M)$.

COROLLARY 11.13. *Suppose M is a finite $G_{\mathbf{Q}_p}$-module of order relatively prime to p. Then, the order of the finite abelian group $H^0(\mathbf{Q}_p, M)$ is the same as that of $H^1_f(\mathbf{Q}_p, M)$.*

PROOF. Since we have $H^0(\mathbf{Q}_p, M) = H^0(\mathbf{F}_p, M^{I_p})$, it suffices to apply Lemma 11.12(1) to the $G_{\mathbf{F}_p}$-module M^{I_p}. ☐

Let p be an odd prime number, and let R be a finite commutative $\mathbf{Z}_p$-algebra. Let M and N be R-$G_{\mathbf{Q}_p}$-modules, good as representations of $G_{\mathbf{Q}_p}$. Through the injection (11.5), we identify the Galois cohomology group $H^1(\mathbf{Q}_p, \operatorname{Hom}_R(M, N))$ with a submodule of

$\mathrm{Ext}_{R\text{-}G_{\mathbf{Q}_p}}(M,N)$. Define the unramified part $H^1_f(\mathbf{Q}_p, \mathrm{Hom}_R(M,N))$ of $H^1(\mathbf{Q}_p, \mathrm{Hom}_R(M,N))$ as the subgroup consisting of the isomorphism classes of extensions good as $G_{\mathbf{Q}_p}$ representations. Considering R as the trivial representation of $G_{\mathbf{Q}_p}$ and identifying N with $\mathrm{Hom}_R(R,N)$, we define a subgroup $H^1_f(\mathbf{Q}_p,N)$ of $H^1(\mathbf{Q}_p,N)$.

LEMMA 11.14. *Let p be an odd prime, and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbf{Q}_p$. Let $n \geq 1$ be an integer, and let $R = \mathcal{O}/\mathfrak{m}^n_{\mathcal{O}}$. Let M and N be finite R-$G_{\mathbf{Q}_p}$-modules. Suppose M is a free R-module, and suppose M and N are good as representations of $G_{\mathbf{Q}_p}$. Let $D(M)$ and $D(N)$ be the strongly divisible filtered φ-R-modules corresponding to M and N, respectively. Then, we have*

$$\frac{\sharp H^1_f(\mathbf{Q}_p, \mathrm{Hom}_R(M,N))}{\sharp \mathrm{Hom}_{R\text{-}G_{\mathbf{Q}_p}}(M,N)} = \sharp \mathrm{Hom}_R(D(M)', D(N)/D(N)').$$

In particular, if $M = R$, we have

$$\frac{\sharp H^1_f(\mathbf{Q}_p, N)}{\sharp H^0(\mathbf{Q}_p, N)} = \sharp D(N)/D(N)'.$$

PROOF. Clear from Corollary C.10. □

EXAMPLE 11.15. Let p be a prime number, and let $n \geq 1$ be an integer.

(1) Suppose $M = \mathbf{Z}/n\mathbf{Z}$. The unramified part $H^1_f(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z})$ of $H^1(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z}) = \mathrm{Hom}(G_{\mathbf{Q}_p}, \mathbf{Z}/n\mathbf{Z})$ is $\{\chi \in \mathrm{Hom}(G_{\mathbf{Q}_p}, \mathbf{Z}/n\mathbf{Z}) \mid \chi(I_p) = 0\} = \mathrm{Hom}(G_{\mathbf{Q}_p}/I_p, \mathbf{Z}/n\mathbf{Z}) = \mathrm{Hom}(G_{\mathbf{F}_p}, \mathbf{Z}/n\mathbf{Z})$.

(2) If $M = \mu_n$, we identify $H^1(\mathbf{Q}_p, \mu_n) = \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n$, Then, we have $H^1_f(\mathbf{Q}_p, \mu_n) = \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$. If n and p are relatively prime, the orders of $H^0(\mathbf{Q}_p, \mu_n)$ and $H^1_f(\mathbf{Q}_p, \mu_n)$ are both equal to the greatest common divisor $(n, p-1)$. If $p \geq 3$ and n is a power of p, then we have $H^0(\mathbf{Q}_p, \mu_n) = 0$, and the order of $H^1_f(\mathbf{Q}_p, \mu_n)$ is n.

LEMMA 11.16. *Let p be a prime number, and let n be a power of p. Let R be a finite commutative $\mathbf{Z}/n\mathbf{Z}$-algebra, let $\alpha : G_{\mathbf{Q}_p} \to R^\times$ be an unramified character, and let N be an R-$G_{\mathbf{Q}_p}$-module obtained from the R-module R by defining the action of $G_{\mathbf{Q}_p}$ by α. Let $\mathbf{Q}_p^{\mathrm{ur}}$ be the maximal unramified extension of $\mathbf{Q}_p$. Then, the natural isomorphism* (11.7) *induces an isomorphism*

$$(\mathbf{Q}_p^{\mathrm{ur}\times}/(\mathbf{Q}_p^{\mathrm{ur}\times})^n \otimes_{\mathbf{Z}/n\mathbf{Z}} N)^{\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ur}}/\mathbf{Q}_p)} \longrightarrow H^1(\mathbf{Q}_p, N(1)). \tag{11.9}$$

By the isomorphism (11.9), *the unramified part* $H^1_f(\mathbf{Q}_p, N(1))$ *is the image of the subgroup* $(\mathbf{Z}_p^{\mathrm{ur}\times}/(\mathbf{Z}_p^{\mathrm{ur}\times})^n \otimes_{\mathbf{Z}/n\mathbf{Z}} N)^{\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ur}}/\mathbf{Q}_p)}$ *of the left-hand side.*

PROOF. The invariant subgroup by the inertia group $N(1)^{I_p}$ is 0. Thus, similarly to Proposition 11.5, the restriction $H^1(\mathbf{Q}_p, N(1)) \to H^1(\mathbf{Q}_p^{\mathrm{ur}}, N(1))^{\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ur}}/\mathbf{Q}_p)}$ is an isomorphism. $H^1(\mathbf{Q}_p^{\mathrm{ur}}, N(1))$ is identified with $\mathbf{Q}_p^{\mathrm{ur}\times}/(\mathbf{Q}_p^{\mathrm{ur}\times})^n \otimes_{\mathbf{Z}/n\mathbf{Z}} N$ by Proposition 11.11(1), and we obtain the isomorphism (11.9).

Define the unramified part $H^1_f(\mathbf{Q}_p^{\mathrm{ur}}, N(1)) \subset H^1(\mathbf{Q}_p^{\mathrm{ur}}, N(1))$ just as $H^1_f(\mathbf{Q}_p, N(1))$. Then, the subgroup $H^1_f(\mathbf{Q}_p^{\mathrm{ur}}, \mu_n) \subset H^1(\mathbf{Q}_p^{\mathrm{ur}}, \mu_n) = \mathbf{Q}_p^{\mathrm{ur}\times}/(\mathbf{Q}_p^{\mathrm{ur}\times})^n$ equals $\mathbf{Z}_p^{\mathrm{ur}\times}/(\mathbf{Z}_p^{\mathrm{ur}\times})^n$. Since $H^1_f(\mathbf{Q}_p, N(1))$ is the inverse image of $H^1_f(\mathbf{Q}_p^{\mathrm{ur}}, N(1))^{\mathrm{Gal}(\mathbf{Q}_p^{\mathrm{ur}}/\mathbf{Q}_p)}$, the assertion follows. ☐

COROLLARY 11.17. *Let p be an odd prime number, and let R be a finite commutative $\mathbf{Z}_p$-algebra. Let $\alpha, \beta : G_{\mathbf{Q}_p} \to R^\times$ be unramified characters, and let M and N be R-$G_{\mathbf{Q}_p}$-modules obtained from the R-module R by defining the action of $G_{\mathbf{Q}_p}$ by α and β, respectively. Let $\mathbf{F}$ be the residue field of R, and let $\overline{M} = M \otimes_R \mathbf{F}$, $\overline{N} = N \otimes_R \mathbf{F}$. If $\alpha \neq \beta$, the image of the natural map $H^1(\mathbf{Q}_p, \mathrm{Hom}_R(M, N(1))) \to H^1(\mathbf{Q}_p, \mathrm{Hom}_{\mathbf{F}}(\bar{M}, \bar{N}(1)))$ is contained in $H^1_f(\mathbf{Q}_p, \mathrm{Hom}_{\mathbf{F}}(\bar{M}, \bar{N}(1)))$.*

PROOF. Replacing α, β by $1, \alpha^{-1}$, we may assume $M = R$. By Lemma 11.16, we have a commutative diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & H^1_f(\mathbf{Q}_p, N(1)) \arrow[r] \arrow[d] & H^1(\mathbf{Q}_p, N(1)) \arrow[r] \arrow[d] & H^0(\mathbf{Q}_p, N) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^1_f(\mathbf{Q}_p, \overline{N}(1)) \arrow[r] & H^1(\mathbf{Q}_p, \overline{N}(1)) \arrow[r] & H^0(\mathbf{Q}_p, \overline{N}) \arrow[r] & 0.
\end{tikzcd}$$

If $\beta \neq 1$, we have $H^0(\mathbf{Q}_p, N) \subsetneq N$, and by Nakayama's lemma, $H^0(\mathbf{Q}_p, N) \to H^0(\mathbf{Q}_p, \bar{N}) \subset \bar{N}$ is the 0 mapping. ☐

Let $n \geq 1$ be an integer, and $M = \mu_n$. By the natural isomorphism $\mathrm{Br}(\mathbf{Q}_p) \to \mathbf{Q}/\mathbf{Z}$ (Theorem 8.25 in *Number Theory 2*), we have a natural isomorphism

$$\frac{1}{n}\mathbf{Z}/\mathbf{Z} \longrightarrow {}_n\mathrm{Br}(\mathbf{Q}_p) \longrightarrow H^2(\mathbf{Q}_p, \mu_n).$$

Let $f : A \times B \to \frac{1}{n}\mathbf{Z}/\mathbf{Z}$ be a bilinear mapping of finite $\mathbf{Z}/n\mathbf{Z}$-modules. For a submodule A' of A, the submodule of B defined as $\{y \in B \mid f(x, y) = 0 \text{ for all } x \in A'\}$ is called the *annihilator* of A'.

PROPOSITION 11.18. *Let p be a prime number, let $n \geq 1$ be an integer, and let M be a finite $\mathbf{Z}/n\mathbf{Z}$-$G_{\mathbf{Q}_p}$-module.*

(1) *$H^0(\mathbf{Q}_p, M)$, $H^1(\mathbf{Q}_p, M)$, and $H^2(\mathbf{Q}_p, M)$ are finite abelian groups. If $q > 2$, we have $H^q(\mathbf{Q}_p, M) = 0$.*

(2) *For an integer $q \geq 0$, the linear mapping*

$$H^q(\mathbf{Q}_p, M) \longrightarrow H^{2-q}(\mathbf{Q}_p, M^\vee(1))^\vee \tag{11.10}$$

defined by the cup product

$$H^q(\mathbf{Q}_p, M) \times H^{2-q}(\mathbf{Q}_p, M^\vee(1)) \longrightarrow H^2(\mathbf{Q}_p, \mu_n) \longrightarrow \frac{1}{n}\mathbf{Z}/\mathbf{Z}$$

is an isomorphism.

(3) *Suppose n is relatively prime to p. Then, the annihilator of the subgroup $H^1_f(\mathbf{Q}_p, M)$ of $H^1(\mathbf{Q}_p, M)$ with respect to the bilinear mapping $H^1(\mathbf{Q}_p, M) \times H^1(\mathbf{Q}_p, M^\vee(1)) \to \frac{1}{n}\mathbf{Z}/\mathbf{Z}$ equals $H^1_f(\mathbf{Q}_p, M^\vee(1))$.*

We do not prove this proposition.

EXAMPLE 11.19. Let $n \geq 1$ be an integer. The isomorphism for $q = 1$ and $M = \mu_n$, $H^1(\mathbf{Q}_p, \mu_n) \to H^1(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z})^\vee$ (11.10) gives the isomorphism of local class field theory

$$\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n \longrightarrow G_{\mathbf{Q}_p}^{\mathrm{ab}}/(G_{\mathbf{Q}_p}^{\mathrm{ab}})^n$$

by the isomorphisms (11.6) and (11.7). If $p \nmid n$, the annihilator of the unramified part $H^1_f(\mathbf{Q}_p, \mu_n) = \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^n$ is the unramified part $H^1_f(\mathbf{Q}_p, \mathbf{Z}/n\mathbf{Z}) = \{\chi \in \mathrm{Hom}(G_{\mathbf{Q}_p}, \mathbf{Z}/n\mathbf{Z}) | \chi(I_p) = 0\}$.

We have the following for the order of the p-adic cohomology group $H^q(G_{\mathbf{Q}_p}, M)$.

PROPOSITION 11.20. *Let M be a finite $G_{\mathbf{Q}_p}$-module. Then we have*

$$\frac{\sharp H^1(\mathbf{Q}_p, M)}{\sharp H^0(\mathbf{Q}_p, M) \cdot \sharp H^2(\mathbf{Q}_p, M)} = \sharp(M \otimes \mathbf{Z}_p).$$

We do not prove this proposition, either.

EXAMPLE 11.21. By the exact sequence

$$0 \longrightarrow H^0(\mathbf{Q}_p, \mu_n) \to \mathbf{Q}_p^\times \xrightarrow{n\text{th power}} \mathbf{Q}_p^\times \to H^1(\mathbf{Q}_p, \mu_n) \longrightarrow 0$$

and the natural isomorphism $\frac{1}{n}\mathbf{Z}/\mathbf{Z} \to H^2(\mathbf{Q}_p, \mu_n)$, we have

$$\frac{\sharp H^1(\mathbf{Q}_p, \mu_n)}{\sharp H^0(\mathbf{Q}_p, \mu_n) \cdot \sharp H^2(\mathbf{Q}_p, \mu_n)} = \frac{n \cdot \sharp \mathbf{Z}_p/n\mathbf{Z}_p}{n} = p \text{ power part of } n.$$

This equals the order of $\mu_n \otimes \mathbf{Z}_p$.

Finally, we consider the case where F is the rational number field $\mathbf{Q}$. For a finite set of prime numbers S, let $\mathbf{Q}_S$ be the compositum of all the subfields of $\overline{\mathbf{Q}}$ that are unramified outside S. Let $G_S = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$. G_S is the quotient of the absolute Galois group $G_{\mathbf{Q}}$ by the closed normal subgroup generated by the images of the inertia groups I_p, $p \notin S$.

Let M be a finite $G_{\mathbf{Q}}$-module. Let S be a finite set of prime numbers such that M is unramified outside S. Then, the action of $G_{\mathbf{Q}}$ on M induces an action of G_S, and M is regarded as a G_S-module naturally.

LEMMA 11.22. *Let M be a finite $G_{\mathbf{Q}}$-module, and let S be a finite set of prime numbers such that M is unramified outside S. Then, we have*

$$H^1(G_S, M) = \mathrm{Ker}\Big(H^1(\mathbf{Q}, M) \to \prod_{\substack{p:\text{prime} \\ p \notin S}} H^1(I_p, M)\Big).$$

PROOF. Let $N = \mathrm{Ker}(G_{\mathbf{Q}} \to G_S)$. The action of N on M is trivial by assumption. Thus, by Proposition 11.5, we obtain an exact sequence $0 \to H^1(G_S, M) \to H^1(\mathbf{Q}, M) \to H^1(N, M) = \mathrm{Hom}(N, M)$. Since N is the closed normal subgroup generated by the image of the inertia groups I_p for prime numbers p not in S, $\mathrm{Hom}(N, M) \to \prod_{p \notin S} \mathrm{Hom}(I_p, M)$ is injective, which proves the assertion. □

COROLLARY 11.23. *Assume furthermore that the order of M is invertible outside S. If $S' \supset S$ is a finite set of prime numbers, we have*

$$H^1(G_S, M) = \mathrm{Ker}\Big(H^1(G_{S'}, M) \to \bigoplus_{p \in S' - S} H^1(\mathbf{Q}_p, M)/H^1_f(\mathbf{Q}_p, M)\Big).$$

PROOF. It follows immediately from Lemma 11.22 and the definition of $H^1_f(\mathbf{Q}_p, M)$. □

EXAMPLE 11.24. Let $n \geq 1$ be an integer, and let S be a finite set of prime numbers containing all the prime divisors of n. Let $\mathbf{Z}_S = \mathbf{Z}[\frac{1}{p}, p \in S]$. Then, the group $H^1(G_S, \mu_n)$ is identified with the kernel of $\mathbf{Q}^\times/(\mathbf{Q}^\times)^n \to \prod_{p \notin S} \mathbf{Q}_p^\times/(\mathbf{Z}_p^\times \cdot (\mathbf{Q}_p^\times)^n)$ by Proposition 11.11(1) and Example 11.15(1). From this we obtain a natural isomorphism

$$H^1(G_S, \mu_n) \longrightarrow \mathbf{Z}_S^\times/(\mathbf{Z}_S^\times)^n. \tag{11.11}$$

The natural mapping $H^2(G_S,\mu_n) \to H^2(\mathbf{Q},\mu_n)$ induces an isomorphism

$$H^2(G_S,\mu_n) \longrightarrow \operatorname{Ker}\Big(H^2(\mathbf{Q},\mu_n) \to \bigoplus_{p\notin S} H^2(\mathbf{Q}_p,\mu_n)\Big). \tag{11.12}$$

By the isomorphism (11.8) and the exact sequence

$$0 \longrightarrow \operatorname{Br}(\mathbf{Q}) \longrightarrow \bigoplus_{p:\text{prime}} \operatorname{Br}(\mathbf{Q}_p) \oplus \operatorname{Br}(\mathbf{R}) \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0,$$

(Theorem 8.26(2) in *Number Theory 2*), we obtain a commutative diagram of exact sequences

(11.13)

$$\begin{tikzcd}
0 \arrow[r] & H^2(\mathbf{Q},\mu_n) \arrow[r] & \bigoplus_{p:\text{prime}} \frac{1}{n}\mathbf{Z}/\mathbf{Z} \oplus \frac{1}{\gcd(n,2)}\mathbf{Z}/\mathbf{Z} \arrow[r] & \frac{1}{n}\mathbf{Z}/\mathbf{Z} \arrow[r] & 0 \\
0 \arrow[r] & H^2(G_S,\mu_n) \arrow[r] \arrow[u, hook, "\cup"'] & \bigoplus_{p\in S} \frac{1}{n}\mathbf{Z}/\mathbf{Z} \oplus \frac{1}{\gcd(n,2)}\mathbf{Z}/\mathbf{Z} \arrow[r] \arrow[u, hook, "\cup"'] & \frac{1}{n}\mathbf{Z}/\mathbf{Z} \arrow[r] \arrow[u, equal] & 0.
\end{tikzcd}$$

PROPOSITION 11.25. *Let $n \geq 1$ be an integer, and let M be a finite $\mathbf{Z}/n\mathbf{Z}$-$G_{\mathbf{Q}}$-module. Let S be a finite set of prime numbers such that n is invertible and M is unramified outside S.*

1. *For an integer $q \geq 0$, $H^q(G_S,M)$ is a finite abelian group, and if $q > 2$ and n is odd, we have $H^q(G_S,M) = 0$.*
2. *If n is odd, we have the exact sequence*

(11.14)

$$\begin{aligned}
0 \longrightarrow H^0(G_S,M) &\longrightarrow \bigoplus_{p\in S} H^0(\mathbf{Q}_p,M) \longrightarrow H^2(G_S,M^\vee(1))^\vee \\
\longrightarrow H^1(G_S,M) &\longrightarrow \bigoplus_{p\in S} H^1(\mathbf{Q}_p,M) \longrightarrow H^1(G_S,M^\vee(1))^\vee \\
\longrightarrow H^2(G_S,M) &\longrightarrow \bigoplus_{p\in S} H^2(\mathbf{Q}_p,M) \longrightarrow H^0(G_S,M^\vee(1))^\vee \longrightarrow 0.
\end{aligned}$$

Here, the mapping $H^q(\mathbf{Q}_p,M) \to H^{2-q}(G_S,M^\vee(1))^\vee$ is the composition of the natural isomorphism $H^q(\mathbf{Q}_p,M) \to H^{2-q}(\mathbf{Q}_p,M^\vee(1))^\vee$ (11.10) and the dual of the restriction mapping $H^{2-q}(G_S,M^\vee(1)) \to H^{2-q}(\mathbf{Q}_p,M^\vee(1))$.

We do not give a proof of this proposition. A similar proposition holds for even n, but in that case we need to consider the infinite places, and we omit it here.

EXAMPLE 11.26. Let the notation be as in Example 11.24. By the isomorphism in Lemma 11.4(1), we identify $H^1(G_S,\mathbf{Z}/n\mathbf{Z})^\vee$ with

$G_S^{\mathrm{ab}}/(G_S^{\mathrm{ab}})^n$. The maximal abelian quotient G_S^{ab} of G_S is equal to the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n}; p \in S, n \geq 1)/\mathbf{Q}) = \prod_{p \in S} \mathbf{Z}_p^\times$. If n is odd, by the isomorphism (11.11), the second line of the exact sequence (11.14) for $M = \mu_n$ gives the isomorphism of class field theory

$$\mathrm{Coker}\Big(\mathbf{Z}_S^\times/(\mathbf{Z}_S^\times)^n \to \bigoplus_{p\in S} \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^n\Big) \longrightarrow G_S^{\mathrm{ab}}/(G_S^{\mathrm{ab}})^n.$$

The third line of (11.14) is the bottom line of (11.13).

About the order of the cohomology group $\sharp H^q(G_S, M)$, the following is known.

Proposition 11.27. *Let M be a finite $G_{\mathbf{Q}}$-module. Let S be a finite set of primes such that M is unramified outside S. Then, we have*

$$\frac{\sharp H^1(G_S, M)}{\sharp H^0(G_S, M) \cdot \sharp H^2(G_S, M)} = \frac{\sharp M}{\sharp M^{G_{\mathbf{R}}}}.$$

We do not prove this either.

Example 11.28. Let the notation be as in Example 11.24. From the exact sequence (11.13), we have $\sharp H^2(G_S, \mu_n) = n^{\# S-1} \cdot \gcd(n, 2)$. By the isomorphism (11.11), we obtain an exact sequence

$$0 \longrightarrow H^0(G_S, \mu_n) \longrightarrow \mathbf{Z}_S^\times \xrightarrow{n\text{th power}} \mathbf{Z}_S^\times \longrightarrow H^1(G_S, \mu_n) \longrightarrow 0.$$

Since $\mathbf{Z}_S^\times$ is isomorphic to $\mathbf{Z}^S \oplus \mathbf{Z}/2\mathbf{Z}$, we have

$$\frac{\sharp H^1(G_S, \mu_n)}{\sharp H^0(G_S, \mu_n) \cdot \sharp H^2(G_S, \mu_n)} = \frac{n^{\sharp S}}{n^{\sharp S-1} \gcd(n, 2)} = \frac{n}{\gcd(n, 2)}.$$

This equals $\sharp \mu_n / \sharp \mu_n^{G_{\mathbf{R}}}$.

11.3. Selmer groups

Definition 11.29. Let $n \geq 1$ be an integer, and let M be a finite $\mathbf{Z}/n\mathbf{Z}$-$G_{\mathbf{Q}}$-module. Let S be a finite set of prime numbers such that M is unramified at all the primes outside S, and all the divisors of n are contained in S.

1. A family $L = (L_p)_{p\in S}$ of subgroups $L_p \subset H^1(\mathbf{Q}_p, M)$ is called a *local condition*.
2. Let $L = (L_p)_{p\in S}$ be a local condition. The *Selmer group* $\mathrm{Sel}_L(M)$ of M with respect to L is defined as the inverse image of $\bigoplus_{p\in S} L_p$ by the restriction mapping $H^1(G_S, M) \to \bigoplus_{p\in S} H^1(\mathbf{Q}_p, M)$.

(3) For a local condition $L = (L_p)_{p \in S}$, the *dual local condition* $L^\vee = (L_p^\vee)_{p \in S}$ is defined as the family of $L_p^\vee \subset H^1(\mathbf{Q}_p, M^\vee(1))$ for $p \in S$, where $L_p^\vee$ is the annihilator of L_p with respect to the bilinear mapping $H^1(\mathbf{Q}_p, M) \times H^1(\mathbf{Q}_p, M^\vee(1)) \to \frac{1}{n}\mathbf{Z}/\mathbf{Z}$ in Proposition 11.18(2).

By Proposition 11.25(1), the Selmer group $\mathrm{Sel}_L(M)$ is a finite group. By defnition,

$$\mathrm{Sel}_L(M) = \mathrm{Ker}\Big(H^1(G_S, M) \to \bigoplus_{p \in S} (H^1(\mathbf{Q}_p, M)/L_p)\Big).$$

By Lemma 11.22, we have

$$\mathrm{Sel}_L(M)$$

$$= \mathrm{Ker}\left(\begin{array}{l} H^1(\mathbf{Q}, M) \longrightarrow \\ \displaystyle\bigoplus_{p \in S} (H^1(\mathbf{Q}_p, M)/L_p) \oplus \prod_{p \notin S} (H^1(\mathbf{Q}_p, M)/H^1_f(\mathbf{Q}_p, M)) \end{array}\right).$$

For a finite set $S' \supset S$, define a local condition $L' = (L'_p)_{p \in S'}$ by $L'_p = L_p$ for $p \in S$ and $L'_p = H^1_f(\mathbf{Q}_p, M)$ for $p \in S' - S$. Then, we have $\mathrm{Sel}_L(M) = \mathrm{Sel}_{L'}(M)$.

EXAMPLE 11.30. Let the notation be as in Example 11.24. Let $n \geq 1$ be an integer, and let S be a finite set of prime numbers that contains all the prime divisors of n. Define the Selmer group $\mathrm{Sel}(\mu_n)$ of μ_n by defining the local condition $L_p \subset H^1(\mathbf{Q}_p, \mu_n) = \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^{\times n}$ for $p \in S$ to be the unramified part $H^1_f(\mathbf{Q}_p, \mu_n) = \mathbf{Z}_p^\times/(\mathbf{Z}_p^\times)^{\times n}$. By the isomorphism (11.11), we obtain

$$\mathrm{Sel}(\mu_n) = \mathbf{Z}^\times/(\mathbf{Z}^\times)^n = \{\pm 1\}/\{(\pm 1)^n\}.$$

EXAMPLE 11.31. Let E be an elliptic curve over $\mathbf{Q}$, and let $n \geq 1$ be an integer. Let $E[n]$ be the finite $G_{\mathbf{Q}}$-module of n-torsion points of E. Let S be a finite set of prime numbers that contains all the primes at which E does not have good reduction and all the prime divisors of n. Define the local condition $L_p \subset H^1(\mathbf{Q}_p, E[n])$ for $p \in S$ as the image of the natural injection $E(\mathbf{Q}_p)/nE(\mathbf{Q}_p) \to H^1(\mathbf{Q}_p, E[n])$.

The Selmer group $\mathrm{Sel}_L(E[n])$ defined by the local condition $L = (E(\mathbf{Q}_p)/nE(\mathbf{Q}_p))_{p \in S}$ is called the Selmer group of E and is denoted by $\mathrm{Sel}(E, n)$. From the finiteness of $\mathrm{Sel}(E, n)$ and the natural injection $E(\mathbf{Q})/nE(\mathbf{Q}) \to \mathrm{Sel}(E, n)$, we obtain the weak Mordel–Weil theorem (§1.3(b) in *Number Theory 1*), which says $E(\mathbf{Q})/nE(\mathbf{Q})$ is a finite group.

Let E be the elliptic curve $y^2 = x^3 - x$ over $\mathbf{Q}$. E has good reduction at $p \neq 2$. If we let $S = \{2\}$, then G_S-module $E[2]$ is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{\oplus 2}$ and $H^1(G_S, E[2])$ is isomorphic to $(\mathbf{Z}[\frac{1}{2}]^\times/(\mathbf{Z}[\frac{1}{2}]^{\times 2}))^{\oplus 2}$. $\mathrm{Sel}(E, 2)$ is isomorphic to $(\mathbf{Z}^\times/(\mathbf{Z}^{\times 2}))^{\oplus 2} = \{\pm 1\}^{\oplus 2}$, and $E[2](\mathbf{Q}) \to \mathrm{Sel}(E, 2)$ is an isomorphism.

PROPOSITION 11.32. *Let $n \geq 1$ be an odd integer, and let M be a finite $\mathbf{Z}/n\mathbf{Z}$-$G_{\mathbf{Q}}$-module. Let S be a finite set of prime numbers such that M is unramified outside S and S contains all the prime divisors of n. Let $L = (L_p)_{p\in S}$ be a local condition, and let $L' = (L'_p)_{p\in S}$ be a family of subgroups $L'_p \subset L_p$. Then, we have the exact sequence*

$$\begin{array}{cccccc} 0 \longrightarrow & \mathrm{Sel}_{L'}(M) & \longrightarrow & \mathrm{Sel}_L(M) & \longrightarrow & \bigoplus_{p\in S} L_p/L'_p \\ \longrightarrow & \mathrm{Sel}_{L'^\vee}(M^\vee(1))^\vee & \longrightarrow & \mathrm{Sel}_{L^\vee}(M^\vee(1))^\vee & \longrightarrow & 0. \end{array}$$

PROOF. The first line is exact by the definition of Selmer groups. Similarly, we have an exact sequence

$$0 \to \mathrm{Sel}_{L^\vee}(M^\vee(1)) \to \mathrm{Sel}_{L'^\vee}(M^\vee(1)) \to \bigoplus_{p\in S} L'^\vee_p/L^\vee_p.$$

By the definition of dual local condition, $L'^\vee_p/L^\vee_p$ is the dual of L_p/L'_p, we obtain the exact sequence $\bigoplus_{p\in S} L_p/L'_p \to \mathrm{Sel}_{L^\vee}(M^\vee(1))^\vee \to \mathrm{Sel}_{L'^\vee}(M^\vee(1))^\vee \to 0$ by taking the dual.

We show the exactness at $\bigoplus_{p\in S} L_p/L'_p$. Define

$$A = \mathrm{Im}\Big(H^1(G_S, M) \to \bigoplus_{p\in S} H^1(\mathbf{Q}_p, M)\Big),$$
$$B = \mathrm{Im}\Big(H^1(G_S, M^\vee(1)) \to \bigoplus_{p\in S} H^1(\mathbf{Q}_p, M^\vee(1))\Big).$$

By Proposition 11.25(2), A is the annihilator of B with respect to the bilinear mapping $\bigoplus_{p\in S} H^1(\mathbf{Q}_p, M) \times \bigoplus_{p\in S} H^1(\mathbf{Q}_p, M^\vee(1)) \to \frac{1}{n}\mathbf{Z}/\mathbf{Z}$. The image of $\mathrm{Sel}_L(M) \to \bigoplus_{p\in S} L_p/L'_p$ is the image of $A \cap \bigoplus_{p\in S} L_p$. Similarly, the image of $\mathrm{Sel}_{L'^\vee}(M^\vee(1)) \to \bigoplus_{p\in S} L'^\vee_p/L^\vee_p$ is the image of $B \cap \bigoplus_{p\in S} L'^\vee_p$. Thus, the kernel of $\bigoplus_{p\in S} L_p/L'_p \to \mathrm{Sel}_{L'^\vee}(M^\vee(1))^\vee$ is the annihilator of the image of $B \cap \bigoplus_{p\in S} L'^\vee_p$ with respect to the bilinear mapping $\bigoplus_{p\in S} L_p/L'_p \times \bigoplus_{p\in S} L'^\vee_p/L^\vee_p \to \frac{1}{n}\mathbf{Z}/\mathbf{Z}$. Thus, it suffices to show the image of $A \cap \bigoplus_{p\in S} L_p$ is the annihilator of $B \cap \bigoplus_{p\in S} L'^\vee_p$ with respect to the bilinear mapping $\bigoplus_{p\in S} L_p/L'_p \times \bigoplus_{p\in S} L'^\vee_p/L^\vee_p \to \frac{1}{n}\mathbf{Z}/\mathbf{Z}$.

The image of $A \cap \bigoplus_{p \in S} L_p$ is the image of

$$(A \cap \bigoplus_{p \in S} L_p) + \bigoplus_{p \in S} L'_p = \bigoplus_{p \in S} L_p \cap (A + \bigoplus_{p \in S} L'_p).$$

Since $\bigoplus_{p \in S} L_p \cap (A + \bigoplus_{p \in S} L'_p)$ is the annihilator of $\bigoplus_{p \in S} L_p^\vee + (B \cap \bigoplus_{p \in S} L'^\vee_p)$, the image of $A \cap \bigoplus_{p \in S} L_p$ is the annihilator of $B \cap \bigoplus_{p \in S} L'^\vee_p$. This shows the exactness at $\bigoplus_{p \in S} L_p / L'_p$. ☐

PROPOSITION 11.33. *Let $n \geq 1$ be an odd integer, and let M be a finite $\mathbf{Z}/n\mathbf{Z}$-$G_{\mathbf{Q}}$-module. Let S be a finite set of prime numbers such that M is unramified outside S and S contains all the prime divisors of n. Let $L = (L_p)_{p \in S}$ be a local condition, and let $L' = (L'_p)_{p \in S}$ be a family of subgroups $L'_p \subset L_p$. Then, we have*

$$\frac{\sharp \operatorname{Sel}_L(M)}{\sharp \operatorname{Sel}_{L^\vee}(M^\vee(1))} = \frac{\sharp M^{G_S}}{\sharp M^\vee(1)^{G_S}} \cdot \prod_{p \in S} \frac{\sharp L_p}{\sharp M^{G_{\mathbf{Q}_p}}} \cdot \frac{1}{\sharp M^{G_{\mathbf{R}}}}.$$

PROOF. $\operatorname{Sel}_L(M)$ is the kernel of the composition of the mapping in the second line of (11.14) $H^1(G_S, M) \to \bigoplus_{p \in S} H^1(\mathbf{Q}_p, M)$ and the surjection $\bigoplus_{p \in S} H^1(\mathbf{Q}_p, M) \to \bigoplus_{p \in S} H^1(\mathbf{Q}_p, M)/L_p$ by the definition of Selmer group. Moreover, by the definitions of the dual local condition and Selmer group, the dual $\operatorname{Sel}_{L^\vee}(M^\vee(1))^\vee$ is identified with the cokernel of the composition of the inclusion $\bigoplus_{p \in S} L_p \to \bigoplus_{p \in S} H^1(\mathbf{Q}_p, M)$ and the mapping of the second line of (11.14) $\bigoplus_{p \in S} H^1(\mathbf{Q}_p, M) \to H^1(G_S, M^\vee(1))^\vee$. Thus, we obtain the exact sequence by Proposition 11.25(2)

$$\begin{array}{ccccc} & & 0 & \longrightarrow & \operatorname{Sel}_L(M) \\ \longrightarrow & H^1(G_S, M) & \longrightarrow & \bigoplus_{p \in S} H^1(\mathbf{Q}_p, M)/L_p & \longrightarrow & \operatorname{Sel}_{L^\vee}(M^\vee(1))^\vee \\ \longrightarrow & H^2(G_S, M) & \longrightarrow & \bigoplus_{p \in S} H^2(\mathbf{Q}_p, M) & \longrightarrow & H^0(G_S, M^\vee(1))^\vee \longrightarrow 0. \end{array}$$

From this we obtain

$$\frac{\sharp \operatorname{Sel}_L(M)}{\sharp \operatorname{Sel}_{L^\vee}(M^\vee(1))} = \frac{\sharp H^1(G_S, M)}{\sharp H^0(G_S, M^\vee(1)) \cdot \sharp H^2(G_S, M)} \times \prod_{p \in S} \frac{\sharp H^2(\mathbf{Q}_p, M) \cdot \sharp L_p}{\sharp H^1(\mathbf{Q}_p, M)}.$$

By Proposition 11.27, the first factor of the right-hand side equals $\frac{\sharp M^{G_S}}{\sharp M^\vee(1)^{G_S}} \frac{\sharp M}{\sharp M^{G_\mathbf{R}}}$. By Proposition 11.20, the contribution of each $p \in S$ is $\frac{\sharp L_p}{\sharp M^{G_{\mathbf{Q}_p}} \cdot \sharp (M \otimes \mathbf{Z}_p)}$. The equality in question follows immediately from this. $\square$

11.4. Selmer groups and deformation rings

In §5.2, we defined the deformation ring R_Σ. In this section we relate deformation rings and Selmer groups, and we reduce Theorems 5.32(1) and 5.34 to properties concerning Selmer groups, Theorem 11.37 and Proposition 11.38.

As in §5.2, let ℓ be an odd prime number, let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$, and let $\bar{\rho} : G_\mathbf{Q} \to \mathrm{GL}_2(\mathbf{F})$ be a modular semistable irreducible mod ℓ-representation. Let K be a finite extension of $\mathbf{Q}_\ell$ whose residue field is $\mathbf{F}$, and let $f \in \Phi(N_\varnothing)_{K,\bar{\rho}}(K)$ be a primitive form with K coefficients. Let $\mathcal{O}$ be the ring of integers of K. The ℓ-adic representation $\rho = \rho_f : G_\mathbf{Q} \to \mathrm{GL}_2(\mathcal{O})$ associated with f is a lifting of $\bar{\rho}$ to $\mathcal{O}$ of type $\mathcal{D}_\varnothing$. $\rho : G_\mathbf{Q} \to \mathrm{GL}_2(\mathcal{O})$ is unramified outside $S_{\bar{\rho}} \cup \{\ell\}$.

As in Definition 5.5, let Σ be a finite set of prime numbers such that $\Sigma \cap S_{\bar{\rho}} = \varnothing$ and that if $\ell \in \Sigma$, then $\bar{\rho}$ is good and ordinary at ℓ. Let $S_\Sigma = S_{\bar{\rho}} \cup \Sigma \cup \{\ell\}$. $\rho : G_\mathbf{Q} \to \mathrm{GL}_2(\mathcal{O})$ induces a representation of G_{S_Σ} on $\mathcal{O}^2$. We regard $\mathcal{O}^2$ as a G_{S_Σ}-module through ρ and denote it by V. Let $W = \mathrm{End}^0(V) = \{f \in \mathrm{End}(V) | \operatorname{Tr} f = 0\}$. W is a free $\mathcal{O}$-module of rank 3 that possesses a natural action of G_{S_Σ}. Let π be a primitive element of $\mathcal{O}$. For an integer $n \geq 1$, let V_n, W_n be $\mathcal{O}/\pi^n\mathcal{O}$-modules $V/\pi^n V, W/\pi^n W = \mathrm{End}^0(V_n)$, respectively. Let $V_\infty = \varinjlim_n V_n = V \otimes K/\mathcal{O}, W_\infty = \varinjlim_n W_n = W \otimes K/\mathcal{O}$. For $n = 1$, let $V_1 = \bar{V}, W_1 = \overline{W}$.

We now give the local condition that defines the Selmer group. Since $\rho : G_\mathbf{Q} \to \mathrm{GL}_2(\mathcal{O})$ is a lifting of $\bar{\rho}$ of type $\mathcal{D}_\varnothing$, if $\ell \notin S_{\bar{\rho}}$, $\bar{\rho}$ is good, and by Theorem 9.13, ρ is good at ℓ. If $\ell \in S_{\bar{\rho}} \cup \Sigma$, then $\bar{\rho}$ is ordinary at ℓ, and by Theorem 3.52(2) and Proposition 7.11, ρ is ordinary at ℓ. If ρ is good at ℓ, define the subgroup $H^1_f(\mathbf{Q}_\ell, W_n)$ of $H^1(\mathbf{Q}_\ell, W_n)$ by

$$H^1_f(\mathbf{Q}_\ell, W_n) = H^1(\mathbf{Q}_\ell, W_n) \cap H^1_f(\mathbf{Q}_\ell, \mathrm{End}(V_n)).$$

If ρ is ordinary at ℓ, define the subgroup $H^1_s(\mathbf{Q}_\ell, W_n)$ of $H^1(\mathbf{Q}_\ell, W_n)$. Let $V_n^0 \subset V_n$ be the subgroup on which I_ℓ acts as the cyclotomic character. $V_n^0, V_n/V_n^0$ are free $\mathcal{O}/\pi^n\mathcal{O}$-modules of rank 1.

Let $W_n^0 \subset W_n$ be $\{f \in \mathrm{End}^0(V_n) | f(V_n^0) = 0, f(V_n) \subset V_n^0\}$. W_n^0 is also a free $\mathcal{O}/\pi^n\mathcal{O}$-module. Define $H_s^1(\mathbf{Q}_\ell, W_n)$ by

$$H_s^1(\mathbf{Q}_\ell, W_n) = \mathrm{Ker}(H^1(\mathbf{Q}_\ell, W_n) \to H^1(I_\ell, W_n/W_n^0)).$$

DEFINITION 11.34. Define the Selmer group

$$\mathrm{Sel}_\Sigma(W_n) \subset H^1(G_{S_\Sigma}, W_n)$$

by the local condition $L_\Sigma = (L_{\Sigma,p})_{p \in S_\Sigma}$ defined by

$$L_{\Sigma,p} = \begin{cases} H_f^1(\mathbf{Q}_p, W_n) & \text{if } p \neq \ell, p \in S_{\bar\rho}, \\ H^1(\mathbf{Q}_p, W_n) & \text{if } p \neq \ell, p \in \Sigma, \\ H_f^1(\mathbf{Q}_\ell, W_n) & \text{if } p = \ell \notin S_{\bar\rho} \cup \Sigma, \\ H_s^1(\mathbf{Q}_\ell, W_n) & \text{if } p = \ell \in S_{\bar\rho} \cup \Sigma. \end{cases}$$

Define $\mathrm{Sel}_\Sigma(W_\infty) = \varinjlim_n \mathrm{Sel}_\Sigma(W_n)$.

We translate the local condition in terms of infinitesimal deformations.

LEMMA 11.35. *Through the bijection* (11.2), *identify* $Z^1(\mathbf{Q}_p, W_n)$ *with* $\mathrm{Lift}^0_{\mathcal{O}/\pi^n\mathcal{O}\text{-}G_{\mathbf{Q}_p}}(V_n)$. *Let* $c : G_{\mathbf{Q}_p} \to W_n$ *be a* 1*-cocycle, and let* $\widetilde{M}$ *be the corresponding infinitesimal lifting.*

(1) *Suppose* $p \neq \ell, p \in S_{\bar\rho}$. *Then,* $[c]$ *belongs to* $H_f^1(\mathbf{Q}_p, W_n)$ *if and only if* $\widetilde{M}$ *is ordinary.*

(2) *Suppose* $p = \ell \in S_{\bar\rho} \cup \Sigma$. *In this case,* ρ *is ordinary at* ℓ. *Then,* $[c]$ *belongs to* $H_s^1(\mathbf{Q}_p, W_n)$ *if and only if* $\widetilde{M}$ *is ordinary.*

PROOF. (1) Suppose $p \neq \ell, p \in S_{\bar\rho}$. If $\sigma \in I_p$ is a lifting of the generator of $I_p/I_p^\ell[I_p, I_p] \simeq \mathbf{Z}/\ell\mathbf{Z}$, then $\bar\rho(\sigma) \neq 1$. If we take a suitable basis of V_n, the matrix representation of the action of σ is given by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Since the image of $I_p \to \mathrm{Aut}_{\mathcal{O}/\pi^n\mathcal{O}} \widetilde{M}$ is generated by σ, the fact that $\widetilde{M}$ is ordinary means that the matrix representation of σ is given by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ if we choose a suitable basis of $\widetilde{M}$. This implies that the infinitesimal lifting $\widetilde{M}$ is isomorphic to $V_n \otimes_{\mathcal{O}/\pi^n\mathcal{O}} \mathcal{O}/\pi^n\mathcal{O}[\varepsilon]$ as $\mathcal{O}/\pi^n\mathcal{O}[\varepsilon]$-$I_p$-modules, which is in turn equivalent to the condition that the restriction of $[c]$ to I_p is 0.

(2) Suppose $p = \ell \in S_{\bar\rho} \cup \Sigma$. In this case, as we remarked above, the restriction of ρ to I_p is ordinary by Proposition 7.11. The part V_n^0 on which the inertia group I_p acts as the cyclotomic character is a free $\mathcal{O}/\pi^n$-module of rank 1. If $c|_{I_p} \in Z^1(I_p, W_n^0)$, then I_p acts on $V_n^0 \otimes_{\mathcal{O}/\pi^n\mathcal{O}} \mathcal{O}/\pi^n O[\varepsilon]$ as the cyclotomic character, and it acts trivially

on $(V_n/V_n^0) \otimes_{\mathcal{O}/\pi^n\mathcal{O}} \mathcal{O}/\pi^n\mathcal{O}[\varepsilon]$. Thus, $\widetilde{M}$ is ordinary. Conversely, suppose $\widetilde{M}$ is ordinary. Then, I_p acts on the submodule $\widetilde{M}^0$ of rank 1 of $\widetilde{M}$ as the cyclotomic character, and it acts trivially on the quotient $\widetilde{M}/\widetilde{M}^0$. Thus if we choose a suitable basis of $\widetilde{M}$, we have $c|_{I_p} \in Z^1(I_p, W_n^0)$. ☐

We give a relation between deformation rings and Selmer groups. Let R_Σ be the deformation ring defined in §5.2, and $\pi_\Sigma : R_\Sigma \to \mathcal{O}$ the homomorphism defined by ρ.

PROPOSITION 11.36. *Let* $\mathfrak{m}_{R_\Sigma}$ *be the maximal ideal of the deformation ring* R_Σ. *Then, there is a natural isomorphism of* $\mathbf{F}$*-linear spaces*

$$\mathrm{Hom}_{\mathbf{F}}(\mathfrak{m}_{R_\Sigma}/(\mathfrak{m}_{R_\Sigma}^2, \pi), \mathbf{F}) \longrightarrow \mathrm{Sel}_\Sigma(\overline{W}). \tag{11.15}$$

Let $\mathfrak{p}_{R_\Sigma}$ *be the kernel of the ring homomorphism* $R_\Sigma \to \mathcal{O}$ *defined by* $\rho : G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathcal{O})$. *Then, there is a natural isomorphism of* $\mathcal{O}$*-modules*

$$\mathrm{Hom}_{\mathcal{O}}(\mathfrak{p}_{R_\Sigma}/\mathfrak{p}_{R_\Sigma}^2, K/\mathcal{O}) \longrightarrow \mathrm{Sel}_\Sigma(W_\infty). \tag{11.16}$$

PROOF. For an integer $n \geq 1$, define a natural injection

$$\mathrm{Hom}_{\mathcal{O}/(\pi^n)}(\mathfrak{p}_{R_\Sigma}/(\mathfrak{p}_{R_\Sigma}^2, \pi^n), \mathcal{O}/(\pi^n)) \longrightarrow H^1(G_{S_\Sigma}, W_n). \tag{11.17}$$

First, we identify $\mathrm{Hom}_{\mathcal{O}/(\pi^n)}(\mathfrak{p}_{R_\Sigma}/(\mathfrak{p}_{R_\Sigma}^2, \pi^n), \mathcal{O}/(\pi^n))$ with a subset of $\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])$. Let $p_n : \mathcal{O}/(\pi^n)[\varepsilon] \to \mathcal{O}/(\pi^n)$ be the natural surjection. If $f : R_\Sigma \to \mathcal{O}/(\pi^n)[\varepsilon]$ is a morphism of $\mathcal{O}$-algebras satisfying $p_n \circ f = \pi_\Sigma \bmod \pi^n$, then the restriction of f to $\mathfrak{p}_{R_\Sigma} = \mathrm{Ker}(\pi_\Sigma : R_\Sigma \to \mathcal{O})$ induces an $\mathcal{O}/(\pi^n)$-linear mapping $\mathfrak{p}_{R_\Sigma}/(\mathfrak{p}_{R_\Sigma}^2, \pi^n) \to \mathcal{O}/(\pi^n)\varepsilon$. By this correspondence, $\mathrm{Hom}_{\mathcal{O}/(\pi^n)}(\mathfrak{p}_{R_\Sigma}/(\mathfrak{p}_{R_\Sigma}^2, \pi^n), \mathcal{O}/(\pi^n))$ is identified with the set

$$\{f : R_\Sigma \to \mathcal{O}/(\pi^n)[\varepsilon] \mid$$
$$f \text{ is a morphism of } \mathcal{O}\text{-algebras with } p_n \circ f = \pi_\Sigma \bmod \pi^n\}$$

This set is identified with the inverse image $\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{[V_n]}$ of the class of V_n by $\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon]) \to \mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n))$ by the definition of the deformation ring R_Σ.

Define $\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$ to be the inverse image of V_n by the mapping $\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon]) \to \mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n))$. Since an element of $\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$ defines an infinitesimal lifting that preserves the determinant of V_n, we obtain a natural injection

$$\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n} \longrightarrow \mathrm{Lift}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n). \tag{11.18}$$

By Proposition 11.8(2), we identify $H^1(G_{S_\Sigma}, W_n)$ with the set of infinitesimal deformations preserving the determinant $\mathrm{Def}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n)$. We show that (11.18) induces an injection

$$\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{[V_n]} \longrightarrow \mathrm{Def}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n). \tag{11.19}$$

The set $\mathrm{Def}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n)$ is the quotient of $\mathrm{Lift}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n)$ by the group $1+\varepsilon\,\mathrm{End}(V_n) = \mathrm{Ker}(\mathrm{GL}_2(\mathcal{O}/(\pi^n)[\varepsilon]) \to \mathrm{GL}_2(\mathcal{O}/(\pi^n))$ by definition. We show $\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{[V_n]}$ is also the quotient of $\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$ by $1+\varepsilon\,\mathrm{End}(V_n)$. For $\rho\in\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$ and $P \in U^1\mathrm{GL}_2(\mathcal{O}/(\pi^n)[\varepsilon]) = \mathrm{Ker}(\mathrm{GL}_2(\mathcal{O}/(\pi^n)[\varepsilon]) \to \mathrm{GL}_2(\mathbf{F}))$, we first show $P \in (1+\mathfrak{m}_{\mathcal{O}/(\pi^n)[\varepsilon]})\cdot(1+\varepsilon\,\mathrm{End}(V_n))$ if $\mathrm{ad}(P)(\rho) \in \mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$. In this case, the image $\overline{P} = P \bmod \varepsilon \in U^1\mathrm{GL}_2(\mathcal{O}/(\pi^n)) = \mathrm{Ker}(\mathrm{GL}_2(\mathcal{O}/(\pi^n)) \to \mathrm{GL}_2(\mathbf{F}))$ satisfies the relation $\mathrm{ad}(\overline{P})(\rho_\Sigma \bmod \pi^n) = \rho_\Sigma \bmod \pi^n$. By the first part of the proof of Proposition 7.15, $M_2(\mathcal{O}/(\pi^n))$ is generated by the image of $\rho_\Sigma \bmod \pi^n$ over $\mathcal{O}/(\pi^n)$. Thus, we have $\overline{P} \in 1+\mathfrak{m}_{\mathcal{O}/(\pi^n)}$, and $P \in (1+\mathfrak{m}_{\mathcal{O}/(\pi^n)[\varepsilon]})\cdot(1+\varepsilon\,\mathrm{End}(V_n))$. Therefore, $\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{[V_n]}$ is the quotient of $\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$ by $(1+\mathfrak{m}_{\mathcal{O}/(\pi^n)[\varepsilon]})\cdot(1+\varepsilon\,\mathrm{End}(V_n))$. Since the action of the scalar matrices $1+\mathfrak{m}_{\mathcal{O}/(\pi^n)[\varepsilon]}$ is trivial, $\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n))[\varepsilon])_{[V_n]}$ is the quotient of $\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$ by $1+\varepsilon\,\mathrm{End}(V_n)$. Hence, $\mathrm{Lift}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n} \to \mathrm{Lift}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n)$ induces an injection $\mathrm{Def}_{\bar\rho,\mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{[V_n]} \to \mathrm{Def}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n)$.

By the natural isomorphism $H^1(G_{S_\Sigma}, W_n) \to \mathrm{Def}^0_{\mathcal{O}/(\pi^n)\text{-}G_{S_\Sigma}}(V_n)$ (11.4), the injection (11.19) defines the injection (11.17). We show the image of the injection (11.17) is $\mathrm{Sel}_\Sigma(W_n)$. It suffices to verify that the ramification condition that a lifting is of type $\mathcal{D}_\Sigma$ corresponds to the local condition that defines the Selmer group for each prime number $p \in S_\Sigma$.

First, suppose $p \neq \ell$. If $p \in S_{\bar\rho}$, the ramification condition is that the lifting is ordinary. Thus, by Lemma 11.35(1), this corresponds to the local condition $H^1_f(\mathbf{Q}_p, W_n)$. If $p \in \Sigma$, there is no ramification condition, which corresponds to the local condition $H^1(\mathbf{Q}_p, W_n)$.

Suppose $p = \ell$. If $\ell \notin S_{\bar\rho}\cup\Sigma$, the ramification condition is that the lifting is good, which corresponds to the local condition $H^1_f(\mathbf{Q}_p, W_n)$. If $\ell \in S_{\bar\rho}\cup\Sigma$, then by Proposition 7.11, the ramification condition is that the lifting is ordinary. Thus, by Lemma 11.35(2), it corresponds to the local condition $H^1_s(\mathbf{Q}_p, W_n)$.

Therefore, the injection (11.17) defines a natural isomorphism $\mathrm{Hom}_{\mathcal{O}/(\pi^n)}(\mathfrak{p}_{R_\Sigma}/(\mathfrak{p}_{R_\Sigma}^2, \pi^n), \mathcal{O}/(\pi^n)) \to \mathrm{Sel}_\Sigma(W_n)$. Letting $n = 1$, we obtain the isomorphism (11.15). Taking $\varinjlim_n$, we obtain the isomorphism (11.16). □

By Proposition 11.36, Theorems 5.32(1) and 5.34 are reduced to Theorem 11.37 and Proposition 11.38, respectively.

THEOREM 11.37. *Let* $r = \dim_{\mathbf{F}} \mathrm{Sel}_\varnothing(\overline{W})$. *For any integer* $n \geq 1$, *there exists a set* Q *consisting of* r *prime numbers* $q_1, \dots, q_r$ *satisfying the condition*

$$(5.19)_n \qquad q_i \notin S_{\bar\rho}, \quad q_i \equiv 1 \bmod \ell^n, \quad \textit{and} \quad \mathrm{Tr}\,\bar\rho(\varphi_{q_i}) \not\equiv \pm 2$$

such that

$$\dim_{\mathbf{F}} \mathrm{Sel}_Q(\overline{W}) = r. \tag{11.20}$$

PROPOSITION 11.38. *Suppose* $p \in \Sigma$, *and let* $\Sigma' = \Sigma - \{p\}$. *Then, we have* $(p+1)^2 - a_p(f)^2 \neq 0$, *and*

$$\mathrm{length}_{\mathcal{O}} \mathrm{Sel}_\Sigma(W_\infty)/\mathrm{Sel}_{\Sigma'}(W_\infty) \leq \mathrm{ord}_{\mathcal{O}}(p-1)((p+1)^2 - a_p(f)^2) \tag{11.21}$$

holds.

We will prove Theorem 11.37 and Proposition 11.38 in §11.6 and §11.5, respectively.

11.5. Calculation of local conditions and proof of Proposition 11.38

In this section we prove Proposition 11.38 by calculating the order of local conditions $H^1_f(\mathbf{Q}_\ell, W_n)$ and $H^1_s(\mathbf{Q}_\ell, W_n)$. The proof of Theorem 11.37, which uses Proposition 11.39 below, will be postponed until the next section. We keep the notation in the previous section. Let M_n be the filtered φ-$\mathcal{O}$-module $D(V_n)$, and define $\mathbf{End}^0_{\mathcal{O}}(M_n) = \mathrm{Ker}(\mathrm{Tr} : \mathbf{Hom}_{\mathcal{O}}(M_n, M_n) \to \mathcal{O}/(\pi^n))$ and its subgroup $\mathbf{End}^0_{\mathcal{O}}(M_n)' = \mathbf{End}^0_{\mathcal{O}}(M_n) \cap \mathbf{Hom}_{\mathcal{O}}(M_n, M_n \to \mathcal{O}/(\pi^n))'$. M_1 is also written $\overline{M}$.

PROPOSITION 11.39. (1) *If* $p \neq \ell$, *then*

$$\dim H^1_f(\mathbf{Q}_p, \overline{W}) = \dim H^0(\mathbf{Q}_p, \overline{W}).$$

(2) *If* $\ell \notin S_{\bar\rho}$, *then*

$$\dim H^1_f(\mathbf{Q}_l, \overline{W}) = \dim H^0(\mathbf{Q}_l, \overline{W}) + 1.$$

(3) *If $\ell \in S_{\bar\rho}$, then*

$$\dim H^1_s(\mathbf{Q}_l, \overline{W}) = \dim H^0(\mathbf{Q}_l, \overline{W}) + 1.$$

PROOF. (1) Clear from Corollary 11.13.

(2) As in the proof of Corollary C.10, we obtain an exact sequence

$$0 \longrightarrow H^0(\mathbf{Q}_\ell, \overline{W}) \longrightarrow \mathbf{End}^0_{\mathbf{F}}(D(\overline{W}))' \longrightarrow \mathbf{End}^0_{\mathbf{F}}(D(\overline{W})) \\ \longrightarrow H^1_f(\mathbf{Q}_\ell, \overline{W}) \longrightarrow 0$$

by Proposition C.9. It now follows from $\dim_{\mathbf{F}} \mathbf{End}^0_{\mathbf{F}}(D(\overline{W})) = 3$ and $\mathbf{End}^0_{\mathbf{F}}(D(\overline{W}))' = 2$.

(3) First, we show

$$H^1_s(\mathbf{Q}_\ell, \overline{W}) = \mathrm{Ker}(H^1(\mathbf{Q}_\ell, \overline{W}) \to H^1(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0)). \tag{11.22}$$

The inclusion $\supset$ is clear. We show $\subset$. Suppose a class M of infinitesimal liftings that preserve the determinant of $\overline{V}$ is contained in $H^1_s(\mathbf{Q}_\ell, \overline{W})$. By Lemma 11.35(2), M is ordinary. If χ is the cyclotomic character, there exists an unramified characters $\alpha, \beta : G_{\mathbf{Q}_\ell} \to \mathbf{F}[\epsilon]^\times$ such that M is the extension of α by $\beta\chi$. Since $\overline{V} = M \otimes_{\mathbf{F}[\epsilon]} \mathbf{F}$ is not good by assumption, we have $\alpha = \beta$ by Corollary 11.17. Since M is an infinitesimal lifting preserving the determinant, we have $\alpha^2 = 1$ and the image of α is contained in $\{\pm 1\} \subset \mathbf{F}^\times$. Thus, by choosing a basis suitably, we may assume that the restriction $c|_{G_{\mathbf{Q}_\ell}}$ of the 1-cocycle c that gives M satisfies $c \in Z^1(G_{\mathbf{Q}_\ell}, \overline{W}^0)$. Thus, we have $[M] \in \mathrm{Ker}(H^1(\mathbf{Q}_\ell, \overline{W}) \to H^1(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0))$, and $H^1_s(\mathbf{Q}_\ell, \overline{W}) = \mathrm{Ker}(H^1(\mathbf{Q}_\ell, \overline{W}) \to H^1(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0))$ is proved.

From the exact sequence

$$0 \longrightarrow H^0(\mathbf{Q}_\ell, \overline{W}^0) \longrightarrow H^0(\mathbf{Q}_\ell, \overline{W}) \longrightarrow H^0(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0) \\ \longrightarrow H^1(\mathbf{Q}_\ell, \overline{W}^0) \longrightarrow H^1(\mathbf{Q}_\ell, \overline{W}) \longrightarrow H^1(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0)$$

and (11.22), we obtain

$$\begin{aligned} &\dim H^1_s(\mathbf{Q}_\ell, \overline{W}) - \dim H^0(\mathbf{Q}_\ell, \overline{W}) \\ &\quad = \dim H^1(\mathbf{Q}_\ell, \overline{W}^0) - \dim H^0(\mathbf{Q}_\ell, \overline{W}^0) - \dim H^0(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0). \end{aligned} \tag{11.23}$$

By Propositions 11.20, and 11.18, the right-hand side of (11.23) is equal to

$$\dim \overline{W}^0 + \dim H^0(\mathbf{Q}_\ell, (\overline{W}^0)^\vee(1)) - \dim H^0(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0).$$

We have $\dim \overline{W}^0 = \dim H^0(\mathbf{Q}_\ell, \overline{W}/\overline{W}^0) = 1$. Since the action of $G_{\mathbf{Q}_\ell}$ on $(\overline{W}^0)^\vee(1)$ is trivial, $\dim H^0(\mathbf{Q}_\ell, (\overline{W}^0)^\vee(1))$ is also 1. Hence, the right-hand side of (11.23) equals 1. □

PROPOSITION 11.40. (1) *Suppose $p \neq \ell$ and $p \notin S_{\bar\rho}$. If $\det(1 - p\varphi_p : W) \neq 0$, then we have*

$$\operatorname{length}_{\mathcal{O}} H^1(\mathbf{Q}_p, W_\infty)/H^1_f(\mathbf{Q}_p, W_\infty) = \operatorname{ord}_{\mathcal{O}} \det(1 - p\varphi_p : W).$$

(2) *Suppose $\bar\rho$ is good and ordinary at ℓ. If $\det(1-\varphi_p : (W^0)^\vee(1)) \neq 0$, then we have*

$$\operatorname{length}_{\mathcal{O}} H^1_s(\mathbf{Q}_\ell, W_\infty)/H^1_f(\mathbf{Q}_\ell, W_\infty) \leq \operatorname{ord}_{\mathcal{O}} \det(1 - \varphi_p : (W^0)^\vee(1)).$$

PROOF. (1) By Proposition 11.18(2), $H^1(\mathbf{Q}_p, W_\infty)/H^1_f(\mathbf{Q}_p, W_\infty)$ is the dual of $H^1_f(\mathbf{Q}_p, W(1))$. Thus, by Lemma 11.12(2), the length of $\mathcal{O}$-module $H^1_f(\mathbf{Q}_p, W(1)) = H^1(\mathbf{F}_p, W(1)) = \operatorname{Coker}(1-\varphi_p : W(1))$ equals $\operatorname{ord}_{\mathcal{O}} \det(1 - p\varphi_p : W)$.

(2) It suffices to show the following:

$$\operatorname{length}_{\mathcal{O}} H^1_f(\mathbf{Q}_\ell, W_n) - \operatorname{length}_{\mathcal{O}} H^0(\mathbf{Q}_\ell, W_n) = n, \tag{11.24}$$

$$\begin{aligned}\operatorname{length}_{\mathcal{O}} H^1_s(\mathbf{Q}_\ell, W_n) &- \operatorname{length}_{\mathcal{O}} H^0(\mathbf{Q}_\ell, W_n) \\ &\leq n + \operatorname{ord}_{\mathcal{O}} \det(1 - \varphi_p : (W^0)^\vee(1)).\end{aligned} \tag{11.25}$$

As in the proof of Proposition 11.39(2), we obtain an exact sequence

$$\begin{aligned}0 \longrightarrow H^0(\mathbf{Q}_\ell, W_n) \longrightarrow \mathbf{End}^0_{\mathcal{O}}(M_n)' \longrightarrow \mathbf{End}^0_{\mathcal{O}}(M_n)& \\ \longrightarrow H^1_f(\mathbf{Q}_\ell, \overline{W}_n) \longrightarrow 0.&\end{aligned}$$

The equality (11.24) follows from the facts $\operatorname{length}_{\mathcal{O}} \mathbf{End}^0_{\mathcal{O}}(M_n) = 3n$ and $\operatorname{length}_{\mathcal{O}} \mathbf{End}^0_{\mathcal{O}}(M_n)' = 2n$.

We show (11.25). $H^1_s(\mathbf{Q}_\ell, W_n)$ is the kernel of the composition $\operatorname{res} \circ u$ of

$$H^1(\mathbf{Q}_\ell, W_n) \xrightarrow{u} H^1(\mathbf{Q}_\ell, W_n/W_n^0) \xrightarrow{\operatorname{res}} H^1(I_\ell, W_n/W_n^0).$$

Since $\operatorname{Ker} \operatorname{res} = H^1(\mathbf{F}_\ell, (W_n/W_n^0)^{I_\ell})$ by Proposition 11.5, we have

$$\operatorname{length}_{\mathcal{O}} H^1_s(\mathbf{Q}_\ell, W_n) \leq \operatorname{length}_{\mathcal{O}} \operatorname{Ker}\ u + \operatorname{length}_{\mathcal{O}} H^1(\mathbf{F}_\ell, (W_n/W_n^0)^{I_\ell}).$$

As in the proof of Proposition 11.39(3), from the exact sequence

$$\begin{aligned}0 \longrightarrow H^0(\mathbf{Q}_\ell, W_n^0) \longrightarrow H^0(\mathbf{Q}_\ell, W_n) \longrightarrow H^0(\mathbf{Q}_\ell, W_n/W_n^0)& \\ \longrightarrow H^1(\mathbf{Q}_\ell, W_n^0) \longrightarrow H^1(\mathbf{Q}_\ell, W_n) \xrightarrow{u} H^1(\mathbf{Q}_\ell, W_n/W_n^0),&\end{aligned}$$

we obtain

$$\begin{aligned}
&\operatorname{length}_{\mathcal{O}} H^1_s(\mathbf{Q}_\ell, W_n) - \operatorname{length}_{\mathcal{O}} H^0(\mathbf{Q}_\ell, W_n)\\
&\quad\leq \operatorname{length}_{\mathcal{O}} H^1(\mathbf{Q}_\ell, W_n^0) - \operatorname{length}_{\mathcal{O}} H^0(\mathbf{Q}_\ell, W_n^0)\\
&\qquad - \operatorname{length}_{\mathcal{O}} H^0(\mathbf{Q}_\ell, W_n/W_n^0) + \operatorname{length}_{\mathcal{O}} H^1(\mathbf{F}_\ell, (W_n/W_n^0)^{I_\ell}).
\end{aligned}$$

The right-hand side equals $\operatorname{length}_{\mathcal{O}} W_n^0 + \operatorname{length}_{\mathcal{O}} H^0(\mathbf{Q}_\ell, (W_n^0)^\vee(1))$ by Lemma 11.12(1) and Proposition 11.20. We have $\operatorname{length}_{\mathcal{O}} W_n^0 = n$, and elementary linear algebra on $\mathcal{O}$-modules shows the inequality $\operatorname{length}_{\mathcal{O}} H^0(\mathbf{Q}_\ell, (W_n^0)^\vee(1)) \leq \operatorname{ord}_{\mathcal{O}} \det(1-\varphi_p : (W^0)^\vee(1))$. Thus, the inequality (11.25) is proved. □

PROOF OF PROPOSITION 11.38. We show the inequality (11.21). First, consider the case $p \neq \ell$. From the exact sequence

$$0 \longrightarrow \operatorname{Sel}_{\Sigma'}(W_\infty) \longrightarrow \operatorname{Sel}_\Sigma(W_\infty) \longrightarrow H^1(\mathbf{Q}_p, W_\infty)/H^1_f(\mathbf{Q}_p, W_\infty),$$

we obtain

$$\begin{aligned}
&\operatorname{length}_{\mathcal{O}} \operatorname{Sel}_\Sigma(W_\infty)/\operatorname{Sel}_{\Sigma'}(W_\infty)\\
&\qquad\qquad\leq \operatorname{length}_{\mathcal{O}} H^1(\mathbf{Q}_p, W_\infty)/H^1_f(\mathbf{Q}_p, W_\infty).
\end{aligned}$$

Thus, by Proposition 11.40(1), it suffices to show

$$\det(1 - p\varphi_p : W) = (1-p)((p+1)^2 - a_p(f)^2) \neq 0. \tag{11.26}$$

Write $1 - a_p(f)t + pt^2 = (1-\alpha t)(1-\beta t)$, and we have

$$(p+1)^2 - a_p(f)^2 = (1+\alpha\beta)^2 - (\alpha+\beta)^2 = (1-\alpha^2)(1-\beta^2). \tag{11.27}$$

By Theorem 9.13, the eigenvalues of $\rho(\varphi_p)$ are α and β. Since $\alpha^2, \beta^2 \neq 1$ by Theorem 9.21, the right-hand side is not 0. Since we have

$$\begin{aligned}
\det(1 - p\varphi_p : W) &= (1-p)(1-p\alpha/\beta)(1-p\beta/\alpha)\\
&= (1-p)(1-\alpha^2)(1-\beta^2),
\end{aligned}$$

the equality in (11.26) is also proved. This completes the proof in the case $p \neq \ell$.

Suppose $p = \ell \in \Sigma$. As in the case $p \neq \ell$, we have

$$\begin{aligned}
&\operatorname{length}_{\mathcal{O}} \operatorname{Sel}_\Sigma(W_\infty)/\operatorname{Sel}_{\Sigma'}(W_\infty)\\
&\qquad\qquad\leq \operatorname{length}_{\mathcal{O}} H^1_s(\mathbf{Q}_p, W_\infty)/H^1_f(\mathbf{Q}_p, W_\infty),
\end{aligned}$$

and $(1-p)((p+1)^2 - a_p(f)^2) \neq 0$. Thus, by Proposition 11.40(2), it suffices to show

$$\operatorname{ord}_{\mathcal{O}} \det(1-\varphi_p : (W^0)^\vee(1)) = \operatorname{ord}_{\mathcal{O}}(1-p)((p+1)^2 - a_p(f)^2). \tag{11.28}$$

Since ρ is ordinary at $p = \ell$, we can write $1 - a_p(f)t + pt^2 = (1 - \alpha t)(1 - p/\alpha \cdot t)$, where α is a p-adic unit by Corollary 9.20(2). Since both $1 - p$ and $1 - (p/\alpha)^2$ are p-adic units, the right-hand side of (11.28) equals $\mathrm{ord}_{\mathcal{O}}(1 - \alpha^2)$ by (11.27). If we denote also by α the unramified character of $G_{\mathbf{Q}_p}$ defined by the property that the image of φ_p is α, the restriction of V to $G_{\mathbf{Q}_p}$ is an extension of α by $\alpha^{-1}(1)$ by Corollary 9.20(2). Thus, we have $W^0 = \mathrm{Hom}(\alpha, \alpha^{-1}(1))$. Hence, $\det(1 - \varphi_p : (W^0)^\vee(1)) = 1 - \alpha^2$. □

11.6. Proof of Theorem 11.37

We first give a summary of group theoretic facts about the absolutely irreducible mod ℓ-representation $\bar{\rho} : G \to \mathrm{GL}_2(\mathbf{F}_\ell)$ that will be needed to prove Theorem 11.37.

PROPOSITION 11.41. *Let ℓ be an odd prime number, and let $G \subset \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ be a finite subgroup. Suppose $V = \overline{\mathbf{F}}_\ell^2$ is absolutely irreducible as a representation of G. Let*

$$W = \mathrm{End}^0(V) = \mathrm{Ker}(\mathrm{Tr}(\mathrm{End}(V) \to \mathbf{F})).$$

Then, one of the following (i) *and* (ii) *holds.*

(i) *W is also absolutely irreducible as a representation of G.*
(ii) *There exist a subgroup H of G of index 2 and a character $\chi : H \to \overline{\mathbf{F}}_\ell^\times$ such that $V \simeq \mathrm{Ind}_H^G \chi$. Let $\delta : G \to G/H \to \{\pm 1\}$ be the character of order 2, and let χ' be the conjugate of χ by $g \in G - H$. Then, we have $\chi' \neq \chi$, and $W \simeq \delta \otimes \mathrm{Ind}_H^G(\chi'/\chi)$.*

PROOF. It suffices to show (ii), assuming W is absolutely reducible. If W is absolutely reducible, W possesses a one- or two-dimensional subspace that is stable under the action of G. Since W is self-dual, we may assume that W has a G-stable one-dimensional subspace T. Let f be a basis of T. Since $\mathrm{Ker}\, f$ is a G-stable subspace of V and V is absolutely irreducible, f defines an isomorphism $V \otimes T \to V$. Let $\delta : G \to \overline{\mathbf{F}}_\ell^\times$ be the character that the action of G on T defines. By the isomorphism $V \otimes T \to V$, we have $\det V \cdot \delta^2 = \det V$, and thus the order of δ is at most 2.

If $\delta = 1$, then the basis f of T defines an endomorphism of V that is not a scalar multiple. Thus, by Schur's lemma, the order of δ is exactly 2. Let $H = \mathrm{Ker}\,\delta$. Again by Schur's lemma, V is reducible as a representation of H. Thus, there exists a character $\chi : H \to \overline{\mathbf{F}}_\ell^\times$

such that $V \simeq \operatorname{Ind}_H^G \chi$. Since V is irreducible, we have $\chi' \neq \chi$. The assertion on W follows immediately from this. ☐

COROLLARY 11.42. *Let the notation be as in Proposition* 11.41. *Then, the following hold.*

(1) $W^G = 0$.
(2) *If* $\delta : G \to \overline{\mathbf{F}}_\ell^\times$ *is a character, then either* (i) *or* (ii) *below holds.*
  (i) $(W \otimes \delta)^G = 0$.
  (ii) *Let* $H = \operatorname{Ker} \delta$. *Then, we have* $[G : H] = 2$, *and there exists a character* $\chi : H \to \overline{\mathbf{F}}_\ell^\times$ *such that* $V \simeq \operatorname{Ind}_H^G \chi$.

PROOF. (1) Clear from Schur's lemma.

(2) Suppose $(W \otimes \delta)^G \neq 0$. Then, there exists a one-dimensional G-stable subspace T of W such that the action of G on T is given by δ^{-1}. As in the proof of Proposition 11.41, we have $\delta^{-1} = \delta$, and the assertion follows from this. ☐

COROLLARY 11.43. *Let the notation be as in Proposition* 11.41. *If* $T \neq 0$ *is a* G*-stable subspace of* W, *then there exists a* $g \in G \subset \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ *that has mutually distinct eigenvalues and that satisfies* $T + (g-1)W = W$.

PROOF. We first show the case where W is absolutely irreducible. In this case we have $T = W$, and it suffices to show that there exists an element g in $G \subset \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ that has distinct eigenvalues. Assuming such a g does not exist, we derive a contradiction. Since V is absolutely irreducible, the center of G is $Z = \{g \in G \mid g \text{ is a scalar matrix}\}$. By the assumption, the order of any element of G/Z is either ℓ or 1. If H is the ℓ-Sylow subgroup of G, we have $G = Z \times H$. Since an irreducible representation of H is one dimensional, this contradicts the irreducibility.

Next, we show the case where W satisfies the condition (ii) of Proposition 11.41. In this case, the order of G is relatively prime to ℓ, the representation W of G is semisimple. By the proof of Proposition 11.41, we may prove it by assuming $T = \delta$ or $T = \operatorname{Ind}_H^G(\chi'/\chi)$ when we decompose $W = \delta \otimes \operatorname{Ind}_H^G(\chi'/\chi)$. If $T = \delta$, we may take a g in H that is not a scalar matrix. If $T = \operatorname{Ind}_H^G(\chi'/\chi)$, we may take a $g \in G - H$. ☐

We give a sufficient condition for $H^1(G, W) = 0$.

LEMMA 11.44. *Let ℓ be an odd prime number, and let $\mathbf{F}$ be a finite extension of $\mathbf{F}_\ell$. If $V = \mathbf{F}^2$ and $W = \mathrm{End}^0(V)$, then we have*

$$H^1(\mathrm{SL}_2(\mathbf{F}), W) = 0$$

except in the case $\mathbf{F} = \mathbf{F}_5$.

OUTLINE OF PROOF. Let $V_0 = \mathbf{F} \subset V$ be a one-dimensional subspace, and define subgroups B and U of $\mathrm{SL}_2(\mathbf{F})$ by $B = \{g \in \mathrm{SL}_2(\mathbf{F}) \mid g(V_0) \subset V_0\} \rhd U = \{g \in B \mid g|_{V_0} = 1\}$. The action on V_0 defines an isomorphism $B/U \to \mathbf{F}^\times$. Explicitly, we have $B = \left\langle \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) \middle| \, a \in \mathbf{F}^\times, u \in \mathbf{F} \right\rangle$ and $U = \{\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right) | \, u \in \mathbf{F}\}$, and the isomorphism $B/U \to \mathbf{F}^\times$ is given by $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) \mapsto a$. Since the indices $[\mathrm{SL}_2(\mathbf{F}) : B]$ and $[B : U]$ are relatively prime to ℓ, the restriction $H^1(\mathrm{SL}_2(\mathbf{F}), W) \to H^1(B, W)$ is injective and $H^1(B, W) \to H^1(U, W)^{B/U}$ is an isomorphism.

Define subspaces of W by $W_1 = \{f \in W | f(V_0) \subset V_0\} \supset W_0 = \{f \in W | f(V_0) = 0\}$. Since the actions of U on W/W_1, W_1/W_0, and W_0 are trivial, $H^1(U, W/W_1)$, $H^1(U, W_1/W_0)$, and $H^1(U, W_0)$ are identified with $\mathrm{Hom}(U, W/W_1)$, $\mathrm{Hom}(U, W_1/W_0)$, and $\mathrm{Hom}(U, W_0)$. Moreover, the invariant parts $H^1(U, W/W_1)^{B/U}$, $H^1(U, W_1/W_0)^{B/U}$, and $H^1(U, W_0)^{B/U}$ are naturally identified with $\mathrm{Hom}_{B/U}(U, W/W_1)$, $\mathrm{Hom}_{B/U}(U, W_1/W_0)$, and $\mathrm{Hom}_{B/U}(U, W_0)$, respectively. We show the following

(i) If $\sharp\mathbf{F} \neq 3, 5, 9$, then $\mathrm{Hom}_{B/U}(U, W/W_1) = 0$.
(ii) If $\sharp\mathbf{F} \neq 3$, then $\mathrm{Hom}_{B/U}(U, W_1/W_0) = 0$.
(iii) $\mathrm{Hom}_{B/U}(U, W_0) = \mathrm{Hom}_{\mathbf{F}}(U, W_0)$.

The isomorphisms of $\mathbf{F}$-vector spaces $W/W_1 \to \mathrm{Hom}_{\mathbf{F}}(V_0, V/V_0)$, $W_1/W_0 \to \mathrm{Hom}_{\mathbf{F}}(V_0, V_0)$, $W_0 \to \mathrm{Hom}_{\mathbf{F}}(V/V_0, V_0)$ are isomorphisms of B/U-modules. Moreover, associating to $g \in U$ the mapping induced by $g - 1$, we obtain an isomorphism of B/U-modules $U \to \mathrm{Hom}_{\mathbf{F}}(V/V_0, V_0)$. Thus, the actions of $B/U = \mathbf{F}^\times$ on W/W_1, W_1/W_0, W_0, U are inverse square, trivial, square, square.

Suppose the order of $\mathbf{F}$ is ℓ^f. We show (i) by contradiction. Suppose $\mathrm{Hom}_{B/U}(U, W/W_1) \neq 0$. There exists a conjugate of the inverse square character of $\mathbf{F}^\times$ that is equal to the square character. Thus, there exists an integer $0 \leq d < f$ satisfying $-2\ell^d \equiv 2 \bmod (\ell^f - 1)$. Since $(\ell^f - 1) \mid 2(\ell^d + 1)$, we have $\ell^f - 1 \leq 2(\ell^d + 1)$, and thus $(\ell^{f-d} - 2)\ell^d \leq 3$. From this we have either $\ell^{f-d} = 3$ and $\ell^d = 1, 3$, or $\ell^{f-d} = 5$ and $\ell^d = 1$. Hence, $\sharp\mathbf{F}$ has to be one of $3, 5, 9$, and (i) is proved. If $\sharp\mathbf{F} \neq 3$, the square mapping is not trivial. (ii) is clear from this. Since $\mathbf{F} = \mathbf{F}_\ell[\mathbf{F}^{\times 2}]$, we have $\mathrm{Hom}_{B/U}(U, W_0) = \mathrm{Hom}_{\mathbf{F}}(U, W_0)$, which shows (iii).

Suppose $\sharp\mathbf{F} \neq 3, 5, 9$, and we show $H^1(U, W)^{B/U}$ that contains $H^1(\mathrm{SL}_2(\mathbf{F}), W)$ itself is 0. By (i), (ii), (iii) above, $\mathrm{Hom}_{\mathbf{F}}(U, W_0) = H^1(U, W_0)^{B/U} \to H^1(U, W)^{B/U}$ is surjective. Consider the long exact sequence

$$H^0(U, W) \longrightarrow H^0(U, W/W_0) \longrightarrow H^1(U, W_0) \longrightarrow H^1(U, W).$$

The first morphism $H^0(U, W) = W_0 \to H^0(U, W/W_0)$ is 0. Therefore, the second morphism induces an isomorphism $H^0(U, W/W_0) = W_1/W_0 \to \mathrm{Hom}_{\mathbf{F}}(U, W_0) = H^1(U, W_0)^{B/U}$. Thus, the morphism $H^1(U, W_0)^{B/U} \to H^1(U, W)^{B/U}$ is 0. Hence, if $\sharp\mathbf{F} \neq 3, 5, 9$, we have $H^1(\mathrm{SL}_2(\mathbf{F}), W) \subset H^1(U, W)^{B/U} = 0$.

Suppose $\sharp\mathbf{F} = 9$. Similarly to the case $\sharp\mathbf{F} \neq 3, 5, 9$, we see that $H^1(U, W)^{B/U} \to H^1(U, W/W_1)^{B/U} = \mathrm{Hom}_{B/U}(U, W/W_1)$ is injective. Moreover, by the proof of (i), $H^1(U, W/W_1)^{B/U}$ is an $\mathbf{F}$-vector space of dimension 1. Suppose there exists an element of $H^1(U, W)^{B/U}$ whose image in $H^1(U, W/W_1)^{B/U}$ is nonzero. On the extension corresponding to this element of the trivial representation $\mathbf{F}$ by W, the actions of $\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ $(a \in \mathbf{F}^\times)$ and $\left(\begin{smallmatrix} 1 & u \\ 0 & 1 \end{smallmatrix}\right)$ $(u \in \mathbf{F})$ are given by

$$\begin{pmatrix} a^2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a^{-2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & u & \frac{u^2}{2} & c(u) \\ 0 & 1 & u & d(u) \\ 0 & 0 & 1 & u^3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

for some functions $c, d : \mathbf{F} \to \mathbf{F}$. There exists no action satisfying such conditions, and thus $H^1(\mathrm{SL}_2(\mathbf{F}), W) \subset H^1(U, W)^{B/U} = 0$ in the case $\sharp\mathbf{F} = 9$, also.

Consider the case $\sharp\mathbf{F} = 3$. It suffices to show $H^1(U, W) = 0$. Since $U \simeq \mathbf{Z}/3\mathbf{Z}$, take its generator σ and we have $H^1(U, W) = \mathrm{Ker}(1 + \sigma + \sigma^2 : W)/\mathrm{Im}(\sigma - 1 : W)$. Since W is isomorphic to $\mathbf{F}[\sigma]/(\sigma - 1)^3$ as an $\mathbf{F}[\sigma]$-module, we have $H^1(U, W) = 0$. □

QUESTION. Fill in the details of the proof of Lemma 11.44.

PROPOSITION 11.45. *Let ℓ be an odd prime number, and let G be a finite subgroup of $\mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ such that $V = \overline{\mathbf{F}}_\ell^2$ is an irreducible representation of G. Let $\delta : G \to \overline{\mathbf{F}}_\ell^\times$ be a character, and let $W = \mathrm{End}^0(V)$. Let $Z = G \cap \overline{\mathbf{F}}_\ell^\times$ be the subgroup of all the scalar matrices* *contained in* G, *and let* $\overline{G} = G/Z$ *be the image of* G *in* $PGL_2(\overline{\mathbf{F}}_\ell) = \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)/\overline{\mathbf{F}}_\ell^\times$. *Then, either* (i), *or* (ii) *holds.*

(i) $H^1(G, W \otimes \delta) = 0$.

(ii) *We have* $\ell = 3$ *or* 5. *If* $\ell = 3$, *then* $\overline{G}$ *is isomorphic to the alternating group* $\mathfrak{A}_5$, *and* $\delta = 1$. *If* $\ell = 5$, *then* $\overline{G}$ *is conjugate to either* $PSL_2(\mathbf{F}_5)$ *or* $PGL_2(\mathbf{F}_5)$, *and* δ *equals either* 1 *or the composition* $(\frac{\det}{5}) = (\frac{}{5}) \circ \det : G \to \overline{G} \to PGL_2(\mathbf{F}_5) \to \mathbf{F}_5^\times/(\mathbf{F}_5^\times)^2 \to \{\pm 1\}$.

We deduce Proposition 11.45 from Theorem 10.28. We first show that for the condition (ii) in Theorem 10.28, the following holds.

LEMMA 11.46. *Let* ℓ *be a prime number, and let* G *be a finite subgroup of* $PGL_2(\overline{\mathbf{F}}_\ell)$. *If* G *is isomorphic to* $PGL_2(\mathbf{F}_\ell)$, *it is conjugate to* $PGL_2(\mathbf{F}_\ell)$, *and if* G *is isomorphic to* $PSL_2(\mathbf{F}_\ell)$, *it is conjugate to* $PSL_2(\mathbf{F}_\ell)$.

PROOF. Consider the natural action of $PGL_2(\overline{\mathbf{F}}_\ell)$ on $\mathbf{P}^1(\overline{\mathbf{F}}_\ell)$. Take an element $g \in G$ of order ℓ. The action of g on $\mathbf{P}^1(\overline{\mathbf{F}}_\ell)$ has only one fixed point, and the orders of all other orbits are all equal to ℓ. Let $X \subset \mathbf{P}^1(\overline{\mathbf{F}}_\ell)$ be a G-orbit containing the g fixed point. The order d of X divides $(\sharp G/\ell) | (\ell^2 - 1)$, and $d \equiv 1 \bmod \ell$. Since $(\ell^2 - 1)/d \equiv -1 \bmod \ell$, we have $(\ell^2 - 1)/d \geq \ell - 1$, and thus $d \leq \ell + 1$. Hence, we have $d = 1$ or $\ell + 1$. If the order of X is 1, G is contained in a conjugate of the image of the group of upper triangular matrices, and thus, it has a normal subgroup of order ℓ, which is a contradiction. This shows the order of X is $\ell + 1$. Choose the coordinates of $\mathbf{P}^1$ such that the fixed point of g is the point at infinity, another point different from this is 0, and $g(0) = 1$. Then, $X = \mathbf{P}^1(\mathbf{F}_\ell)$. Since the action of G sends $0, 1, \infty$ to points in $\mathbf{P}^1(\mathbf{F}_\ell)$, G is a subgroup of $PGL_2(\mathbf{F}_\ell)$ of index less than 2. Since the abelianization of $PGL_2(\mathbf{F}_\ell)$ is of order 2, the only subgroup of index 2 is $PSL_2(\mathbf{F}_\ell)$, if $\ell \neq 2$. ☐

PROOF OF PROPOSITION 11.45. We have an exact sequence $0 \to H^1(\bar{G}, (W \otimes \delta)^Z) \to H^1(G, W \otimes \delta) \to H^1(Z, W \otimes \delta)$ by Proposition 11.5. Since the order of Z is relatively prime to ℓ, we have $H^1(Z, W \otimes \delta) = 0$ by Lemma 11.3. Thus, the natural mapping $H^1(\bar{G}, (W \otimes \delta)^Z) \to H^1(G, W \otimes \delta)$ is an isomorphism. Since the action of Z on W is trivial, we have $(W \otimes \delta)^Z = 0$ if $\delta|_Z \neq 1$.

From now on, suppose $\delta|_Z = 1$, and we identify δ with a character of $\overline{G}$. Furthermore, we identify $H^1(\overline{G}, W \otimes \delta)$ with $H^1(G, W \otimes \delta)$. It suffices to show the assertion in each case where the conditions (i),

(ii) or (iii) in Theorem 10.28 holds. Suppose first condition (iii) holds. In this case, the order of G is relatively prime to ℓ by the assumption $\ell \neq 2$. Thus, by Lemma 11.3, we have $H^1(G, W \otimes \delta) = 0$.

Next, suppose condition (i) holds. Suppose $\overline{G}$ is conjugate to $PSL_2(\mathbf{F})$. We may assume $\overline{G} = PSL_2(\mathbf{F})$ by replacing a basis. Then, we have $\delta = 1$. By Proposition 11.5, $H^1(PSL_2(\mathbf{F}), W) \rightarrow H^1(\mathrm{SL}_2(\mathbf{F}), W)$ is injective. Thus, $H^1(\bar{G}, W \otimes \delta) = H^1(\bar{G}, W) = 0$ by Lemma 11.44 except for the case $\mathbf{F} = \mathbf{F}_5$. Suppose $\overline{G}$ is conjugate to $PGL_2(\mathbf{F})$. If $\overline{H} \subset \overline{G}$ is a subgroup conjugate to $PSL_2(\mathbf{F})$, then $H^1(\bar{G}, W \otimes \delta) \rightarrow H^1(\bar{H}, W \otimes \delta)$ is injective by Proposition 11.5 and Lemma 11.3 as above, and thus $H^1(\bar{G}, W \otimes \delta) = 0$ except for $\mathbf{F} = \mathbf{F}_5$. If $\mathbf{F} = \mathbf{F}_5$, the composition $(\frac{\det}{5}) : PGL_2(\mathbf{F}_5)^{\mathrm{ab}} \rightarrow \mathbf{F}_5^\times/(\mathbf{F}_5^\times)^2 \rightarrow \{\pm 1\}$ is injective, and thus δ is either 1 or $(\frac{\det}{5})$.

Finally, suppose condition (ii) holds. If $\ell > 5$, then the order of G is relatively prime to ℓ, and thus $H^1(G, W \otimes \delta) = 0$ by Lemma 11.3. If $\ell = 3$, the assertion is reduced to the case where condition (i) holds by Lemma 11.46, except for the case in which $\overline{G}$ is isomorphic to $\mathfrak{A}_5$. If $\overline{G} \simeq \mathfrak{A}_5$, we have $\overline{G}^{\mathrm{ab}} = 1$, and thus $\delta = 1$. If $\ell = 5$, except for the case $\overline{G} \simeq \mathfrak{A}_5$, the order of G is relatively prime to ℓ, and thus $H^1(G, W \otimes \delta) = 0$. If $\overline{G}$ is isomorphic to $\mathfrak{A}_5$, $\overline{G}$ is conjugate to $PSL_2(\mathbf{F}_5)$ by Lemma 11.46. ☐

COROLLARY 11.47. *Let the assumption be as in Proposition 11.45. If $\ell \neq 3, 5$ or $\det G \neq 1$, then we have*

$$H^1(G, W \otimes \det) = 0.$$

PROOF. It suffices to show that condition (ii) in Proposition 11.45 does not hold assuming $\ell = 3, 5$ and $\delta = \det \neq 1$. Since $\det \neq 1$, if we assume condition (ii) holds, then we have $\ell = 5$, $\det = (\frac{\det}{5})$ and $\det(G) = \{\pm 1\}$. However, we have $-1 \neq (\frac{-1}{5})$ which is contradiction. ☐

In what follows let the notation be as in the previous section.

PROOF OF THEOREM 11.37. Since $r = \dim \mathrm{Sel}_{\varnothing}(\overline{W})$, the equality $r = \dim \mathrm{Sel}_Q(\overline{W})$ is equivalent to the condition that the inclusion $\mathrm{Sel}_{\varnothing}(\overline{W}) \rightarrow \mathrm{Sel}_Q(\overline{W})$ is an isomorphism. Since $\overline{W}$ is self-dual, $\mathrm{Sel}_{Q^\vee}(\overline{W}(1))^\vee$ is the Selmer group defined by the dual local condition.

By Proposition 11.32, there is an exact sequence

$$0 \longrightarrow \mathrm{Sel}_{\varnothing}(\overline{W}) \longrightarrow \mathrm{Sel}_Q(\overline{W}) \longrightarrow \bigoplus_{p\in Q} H^1(\mathbf{Q}_p, \overline{W})/H^1_f(\mathbf{Q}_p, \overline{W})$$

$$\longrightarrow \mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1))^\vee \longrightarrow \mathrm{Sel}_{Q^\vee}(\overline{W}(1))^\vee \longrightarrow 0.$$

Thus, the equality $r = \dim \mathrm{Sel}_Q(\overline{W})$ is equivalent to the condition that $\bigoplus_{p\in Q} H^1(\mathbf{Q}_p, \overline{W})/H^1_f(\mathbf{Q}_p, \overline{W}) \to \mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1))^\vee$ is injective. It is also equivalent to the condition that

$$\mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1)) \to \bigoplus_{p\in Q} H^1(\mathbf{F}_p, \overline{W}(1))$$

is surjective.

We now show the following lemma.

LEMMA 11.48. (1) $\dim_{\mathbf{F}} \mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1)) = \dim_{\mathbf{F}} \mathrm{Sel}_{\varnothing}(\overline{W}) = r$.
(2) *If a prime number q satisfies the condition*

$$q \notin S_{\bar\rho}, \quad q \equiv 1 \bmod \ell \quad \textit{and} \quad \mathrm{Tr}\,\bar\rho(\varphi_q) \not\equiv \pm 2, \tag{11.29}$$

then we have $\dim_{\mathbf{F}} H^1(\mathbf{F}_q, \overline{W}(1)) = 1$.

PROOF. (1) Apply Proposition 11.33 to $M = \overline{W}$. Since $\overline{W}$ is self-dual, it suffices to verify the following.

(i) $\dim_{\mathbf{F}} H^1(G_{\mathbf{F}_p}, \overline{W}^{I_p}) = \dim_{\mathbf{F}} \overline{W}^{G_{\mathbf{Q}_p}}$ if $p \in S_{\bar\rho}, \neq \ell$,
(ii) $\dim_{\mathbf{F}} H^1_f(G_{\mathbf{Q}_\ell}, \overline{W}) - \dim_{\mathbf{F}} \overline{W}^{G_{\mathbf{Q}_\ell}} = 1$ if $\ell \notin S_{\bar\rho}$,
(iii) $\dim_{\mathbf{F}} H^1_s(G_{\mathbf{Q}_\ell}, \overline{W}) - \dim_{\mathbf{F}} \overline{W}^{G_{\mathbf{Q}_\ell}} = 1$ if $\ell \in S_{\bar\rho}$,
(iv) $\dim_{\mathbf{F}} \overline{W}^{G_{\mathbf{R}}} = 1$,
(v) $\overline{W}^{G_S} = \overline{W}(1)^{G_S} = 0$.

(i), (ii), and (iii) are Proposition 11.39(1), (2), and (3), respectively. (iv) follows from the fact that for a complex conjugate c, $\bar\rho(c)$ has eigenvalues 1 and -1 with multiplicity one. We show (v). Condition (ii) in Corollary 11.42(2) does not hold by Lemma 9.51. Thus, (v) follows from Corollary 11.42.

(2) By the condition (10.22), $\bar\rho(\varphi_q)$ has two distinct eigenvalues. The assertion follows immediately from this. ☐

By Lemma 11.48, $\mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1)) \to \bigoplus_{p\in Q} H^1(\mathbf{F}_p, \overline{W}(1))$ is surjective if and only if it is injective. We show there exists a Q that makes

$$\mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1)) \longrightarrow \bigoplus_{p\in Q} H^1(\mathbf{F}_p, \overline{W}(1)) = \bigoplus_{p\in Q} \overline{W}(1)/(\varphi_p - 1)\overline{W}(1)$$

injective. By Theorem 3.1, it suffices to show there exist $\sigma_1, \dots, \sigma_r \in G_{\mathbf{Q}(\zeta_{\ell^n})}$ such that each $\bar{\rho}(\sigma_i)$ has two distinct eigenvalues, and the direct sum of the restriction mapping

$$\mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1)) \to \bigoplus_{i=1}^{r} \overline{W}(1)/(\sigma_i - 1)\overline{W}(1)$$

is injective. For any nonzero element of $\mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1))$, let $c : G_{\mathbf{Q}} \to \overline{W}(1)$ be a 1-cocycle that represents it. Then, it suffices to show there exists $\sigma \in G_{\mathbf{Q}(\zeta_{\ell^n})}$ such that $\bar{\rho}(\sigma)$ has two distinct eigenvalues, and that $c(\sigma) \in \overline{W}(1)$ is not contained in $(\sigma - 1)\overline{W}(1)$.

Let $G_{F_n} = \mathrm{Ker}(\bar{\rho} : G_{\mathbf{Q}(\zeta_{\ell^n})} \to \mathrm{GL}_2(\mathbf{F}))$. We show the restriction mapping

$$H^1(G_{\mathbf{Q}}, \overline{W}(1)) \to H^1(G_{F_n}, \overline{W}(1)) = \mathrm{Hom}(G_{F_n}, \overline{W}(1)) \tag{11.30}$$

is injective. The kernel equals $H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \overline{W}(1))$ by Proposition 11.5. Thus, it suffices to show $H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \overline{W}(1)) = 0$. Moreover, by Proposition 11.5, we obtain an exact sequence

(11.31)

$$\begin{aligned} 0 &\longrightarrow H^1(\mathrm{Gal}(F_0/\mathbf{Q}), \overline{W}(1)^{\mathrm{Gal}(F_n/F_0)}) \\ &\longrightarrow H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \overline{W}(1)) \longrightarrow H^1(\mathrm{Gal}(F_n/F_0), \overline{W}(1))^{\mathrm{Gal}(F_0/\mathbf{Q})}. \end{aligned}$$

Since $\det \bar{\rho}$ is the mod ℓ cyclotomic character, we have $\mathbf{Q}(\zeta_\ell) \subset F_0$. Thus, the action of $\mathrm{Gal}(F_n/F_0)$ on $\overline{W}(1)$ is trivial. Therefore, it suffices to show the following:

$$\begin{aligned} &H^1(\mathrm{Gal}(F_0/\mathbf{Q}), \overline{W}(1)) = 0, \\ &H^1(\mathrm{Gal}(F_n/F_0), \overline{W}(1))^{\mathrm{Gal}(F_0/\mathbf{Q})} \\ &\qquad\qquad = \mathrm{Hom}_{\mathrm{Gal}(F_0/\mathbf{Q})}(\mathrm{Gal}(F_n/F_0), \overline{W}(1)) = 0. \end{aligned}$$

The determinant $\det \bar{\rho}$ is the mod ℓ cyclotomic character, and is nontrivial. Since $\bar{\rho}$ is an absolutely irreducible faithful representation of $\mathrm{Gal}(F_0/\mathbf{Q})$, by Corollary 11.47, we have $H^1(\mathrm{Gal}(F_0/\mathbf{Q}), \overline{W}(1)) = 0$. We show $\mathrm{Hom}_{\mathrm{Gal}(F_0/\mathbf{Q})}(\mathrm{Gal}(F_n/F_0), \overline{W}(1)) = 0$. Since $F_n = F_0 \cdot \mathbf{Q}(\zeta_{\ell^n})$, $\mathrm{Gal}(F_n/F_0) \to \mathrm{Gal}(\mathbf{Q}(\zeta_{\ell^n})/\mathbf{Q})$ is injective, and the conjugate action of $\mathrm{Gal}(F_0/\mathbf{Q})$ on $\mathrm{Gal}(F_n/F_0)$ is trivial. Therefore, if $f : \mathrm{Gal}(F_n/F_0) \to \overline{W}(1)$ is a morphism of $\mathrm{Gal}(F_0/\mathbf{Q})$-modules, the image of f is contained in the invariant part $\overline{W}(1)^{\mathrm{Gal}(F_0/\mathbf{Q})}$. Hence, we have $\mathrm{Hom}_{\mathrm{Gal}(F_0/\mathbf{Q})}(\mathrm{Gal}(F_n/F_0), \overline{W}(1)) = 0$. This completes the proof of $H^1(\mathrm{Gal}(F_n/\mathbf{Q}), \overline{W}(1)) = 0$, and $H^1(G_{\mathbf{Q}}, \overline{W}(1)) \to \mathrm{Hom}(G_{F_n}, \overline{W}(1))$ is injective.

Take any nonzero element of $\mathrm{Sel}_{\varnothing^\vee}(\overline{W}(1))$, and let $c : G_{\mathbf{Q}} \to \overline{W}(1)$ be a 1-cocycle that represents it. The restriction of c to G_{F_n} defines a homomorphism $c|_{G_{Fn}} : G_{F_n} \to \overline{W}(1)$. Since $H^1(G_{\mathbf{Q}}, \overline{W}(1)) \to \mathrm{Hom}(G_{F_n}, \overline{W}(1))$ is injective, $c(G_{F_n}) \subset \overline{W}(1)$ is not 0. This is a subspace of $\overline{W}(1)$ stable under the action of $G_{\mathbf{Q}(\zeta_{\ell^n})}$. The restriction $\bar{\rho}|_{G_{\mathbf{Q}(\zeta_{\ell^n})}}$ is absolutely irreducible by Corollary 9.52. Thus, by Corollary 11.43, there exists $\sigma \in G_{\mathbf{Q}(\zeta_{\ell^n})}$ such that $\bar{\rho}(\sigma)$ has two distinct eigenvalues, and satisfies $c(G_{F_n}) + (\sigma - 1)\overline{W} = \overline{W}$. If $c(\sigma) \notin (\sigma - 1)\overline{W}$, this $\sigma \in G_{\mathbf{Q}(\zeta_{\ell^n})}$ satisfies the condition. If $c(\sigma) \in (\sigma - 1)\overline{W}$, take $\tau \in G_{F_n}$ such that $c(\tau) \notin (\sigma - 1)\overline{W}$. Since $\bar{\rho}(\sigma) = \bar{\rho}(\sigma\tau)$ and $c(\sigma\tau) = c(\sigma) + \sigma c(\tau) \equiv c(\tau) \not\equiv 0 \bmod (\sigma - 1)\overline{W}$, $\sigma\tau \in G_{\mathbf{Q}(\zeta_{\ell^n})}$ satisfies the condition. □

APPENDIX B

Curves over discrete valuation rings

B.1. Curves

DEFINITION B.1. (1) Let k be a field. A separated scheme X of finite type over k such that each connected component is one dimensional is called a *curve* over k.

If X is a proper smooth curve over k whose geometric fiber is connected, then $g = \dim_k H^1(X, \mathcal{O})$ is called the *genus* of X.

(2) A flat scheme X of finite presentation over a scheme S such that the geometric fiber $X_{\bar{s}}$ for each geometric point $\bar{s} \to S$ is a curve over $\kappa(\bar{s})$ is called a curve over S.

If X is a proper smooth curve over S such that each geometric fiber is connected and of genus g, we say that the genus of X is g.

LEMMA B.2. *Let S be a scheme, and let X be a curve over S.*

(1) *Suppose X is smooth over S. Then, for a closed subscheme D of X finite of finite presentation over S, the following conditions* (i) *and* (ii) *are equivalent.*
  (i) *D is flat over S.*
  (ii) *D is a Cartier divisor of X.*

(2) *If a closed subscheme D of X is a Cartier divisor of S and D is étale over S, then X is smooth over S on a neighborhood of D.*

PROOF. (1) (i) $\Rightarrow$ (ii). Since the assertion is local on S, we may assume that D is of degree $N \geq 1$ over S. We prove by induction on N. First, we show the case $N = 1$. Since the assertion is local on X, we may assume $S = \operatorname{Spec} A$, and there is an étale morphism $X \to \mathbf{A}^1_S = \operatorname{Spec} A[T]$. Thus, we may assume $X = \mathbf{A}^1_S$. But in this case, the assertion is clear.

We show the case in which N is general. Since D is a flat covering of S and the assertion is flat local on S, we may assume that D has a section $P : S \to D$. Since the case $N = 1$ is already shown, P

defines a Cartier divisor of X. Thus, there exists a closed subscheme D' of D such that $\mathcal{I}_{D'} \subset \mathcal{O}_X$ and $\mathcal{I}_P \subset \mathcal{O}_X$ satisfy $\mathcal{I}_D = \mathcal{I}_{D'}\mathcal{I}_P$. Since we have an exact sequence $0 \to \mathcal{O}_{D'} \to \mathcal{O}_D \to \mathcal{O}_S \to 0$ of $\mathcal{O}_D$-modules locally on S, D' is flat over S of degree $N-1$. It follows from the induction hypothesis that D' is a Cartier divisor, and thus so is $D = D' + P$.

(ii) ⇒ (i). The defining ideal $\mathcal{I}_D$ of D is an invertible $\mathcal{O}_X$-module. Since D_s is a finite subscheme of X_s for any point s in S, the ideal $\mathcal{I}_{D,x}\mathcal{O}_{X_s,x} \subset \mathcal{O}_{X_s,x}$ is generated by nonzero divisors for any point x in the smooth curve X_s. In other words, tensoring $\otimes\kappa(s)$ to the exact sequence $0 \to \mathcal{I}_D \to \mathcal{O}_X \to \mathcal{O}_D \to 0$ for each $s \in S$, we obtain an exact sequence $0 \to \mathcal{I}_{D_s} \to \mathcal{O}_{X_s} \to \mathcal{O}_{D_s} \to 0$. Thus, we have $\mathrm{Tor}_1^{\mathcal{O}_S}(\mathcal{O}_D, \kappa(s)) = 0$, and $\mathcal{O}_D$ is a flat $\mathcal{O}_S$-module.

(2) By Proposition A.4(1), we may assume $S = \operatorname{Spec} k$ with k an algebraically closed field. If $x \in D$, then the local ring $\mathcal{O}_{X,x}$ is regular, and the assertion follows from Proposition A.4(2). □

We define an ordinary double point of a curve over a field.

Definition B.3. Let X be a curve over a field k, and let x be a closed point in X. We call x a *node* of X if there exist étale morphisms $u : U \to X$, $f : U \to \operatorname{Spec} k[S,T]/(ST)$ and a point $v \in U$ satisfying $u(v) = x$ and $f(v) = (S,T)$.

Lemma B.4. *Let X be a curve over a field k, and let x be a closed point of X. Then, the following conditions* (i)–(iii) *are equivalent.*

(i) *x is a node.*

(ii) *The residue field $\kappa(x)$ is a finite separable extension of k. X is reduced on a neighborhood of x, and the normalization $\overline{X}$ is smooth over k on a neighborhood of the inverse image of x. The length of the $\mathcal{O}_{X,x}$-module $(\mathcal{O}_{\overline{X}}/\mathcal{O}_X)_x$ is 1, and $\overline{X} \times_X x$ is finite étale over x of degree 2.*

(iii) *If $\bar{k}$ is an algebraic closure of k, the completion $\widehat{\mathcal{O}}_{X_{\bar{k}},\bar{x}}$ of the local ring at each point $\bar{x} \in x \times_k \bar{k} \subset X_{\bar{k}} = X \times_k \bar{k}$ of the inverse image of x is isomorphic to $\bar{k}[[S,T]]/(ST)$ over $\bar{k}$.*

Proof. (i) ⇒ (ii), (iii). The assertion is étale local. Thus, we may assume $X = \operatorname{Spec}[S,T]/(ST)$ and $x = (S,T)$. But in this case, the assertion is clear.

(ii) ⇒ (i). Let $\overline{X} \to X$ be the normalization of X. Replacing k by some finite separable extension if necessary, we may assume x and the points of its inverse image in $\overline{X}$ are k-rational points. Replacing

X by a neighborhood of x, we may assume $X = \operatorname{Spec} A$ is reduced and affine, and its normalization $\overline{X} = \operatorname{Spec} B$ is smooth over k.

Let x_1, x_2 be the inverse images of x. We first show the case where the normalization $\overline{X}$ is decomposed into a disjoint union $V_1 \coprod V_2 = \operatorname{Spec} B_1 \times B_2$ ($x_i \in V_i$). In this case A is the inverse image of the diagonal subring $k \subset k \times k$ by the surjection $B_1 \times B_2 \to k \times k$ defined by x_1 and x_2. Thus, if we let $S \in B_1$ and $T \in B_2$ be prime elements at x_1 and x_2, respectively, we obtain a ring homomorphism $k[S,T]/(ST) \to A$. The morphism $X \to \operatorname{Spec} k[S,T]/(ST)$ defined by it is étale on a neighborhood of x.

We deduce the general case from the previous case. Let $\mathfrak{m}$ be the maximal ideal of A corresponding to x. Then, we have $\mathfrak{m}B = \mathfrak{m}$, and $B/\mathfrak{m}B$ is isomorphic to $k \times k$. Take an element b in B such that its image in $k \times k$ is $(1,0)$, and let $a = b^2 - b \in \mathfrak{m}B = \mathfrak{m} \subset A$. Furthermore, let $g(Y) = Y^2 - Y - a \in A[Y]$, let $\tilde{A} = A[Y]/g(Y)$, and let $U = \operatorname{Spec} \tilde{A}$. Since $u : U \to X$ is flat, and the fiber at x is étale, we may assume $U \to X$ is étale by replacing X by a neighborhood of x if necessary. By Proposition A.13(3), $U \times_X \overline{X}$ is a normalization of U. Since the étale covering $U \times_X \overline{X} \to \overline{X}$ of degree 2 has a section defined by the homomorphism $\tilde{A} = A[Y]/g(Y) \to B : Y \mapsto b$, it is isomorphic to $\overline{X} \coprod \overline{X}$. Thus, the general case is reduced to the case where the normalization $\overline{X}$ is decomposed into the disjoint union $V_1 \coprod V_2$.

(iii) ⇒ (ii). We prove it assuming k is a perfect field. In this case, replacing k by $\bar{k}$, we may assume k is algebraically closed. Since the local ring $\mathcal{O}_{X,x}$ is a subring of the completion $\widehat{\mathcal{O}}_{X,x}$, it is reduced. Thus, replacing X by a neighborhood of x, we may assume X is reduced. The normalization $\overline{X}$ is smooth over k. If we identify the completion of $\mathcal{O}_{X,x}$ with $k[[S,T]]/(ST)$, the completion of $\mathcal{O}_{\overline{X}}$ at the inverse image of x in $\overline{X}$ is $k[[S]] \times k[[T]]$. Thus, the remaining assertion follows easily. □

We define the dual chain complex for a proper curve over a perfect field.

Definition B.5. Let k be a perfect field, and let X be a proper curve over k. Let $\bar{k}$ be an algebraic closure of k.

First, suppose X is reduced. Let $\overline{X}$ be the normalization of X. We call $P = \operatorname{Spec} \Gamma(\overline{X}, \mathcal{O})$ the finite scheme consisting of irreducible components of X. Let Σ be the reduced closed subscheme of X consisting of all the singular points, and $\overline{\Sigma} = \overline{X} \times_X \Sigma$. Let $\Gamma_0 = \mathbf{Z}^{P(\bar{k})}$, and let Γ_1 be the kernel of the surjective homomorphism

$\mathbf{Z}^{\overline{\Sigma}(\bar{k})} \to \mathbf{Z}^{\Sigma(\bar{k})}$ defined by the natural morphism $\overline{\Sigma} \to \Sigma$. Let $d : \Gamma_1 \to \Gamma_0$ be the homomorphism defined by the natural morphism $\overline{\Sigma} \to \overline{X}$. Then, we call the chain complex $\Gamma = [\Gamma_1 \to \Gamma_2]$ of length 1 the *dual chain complex* of X.

For a general X, we define the dual chain complex of X as the dual chain complex of the reduced part of X.

The condition that $H_0(\Gamma) = \mathbf{Z}$ is equivalent to the condition that the geometric fiber $X_{\bar{k}}$ is connected.

B.2. Semistable curve over a discrete valuation ring

In what follows, let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field.

DEFINITION B.6. Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field.

(1) Let X be a flat curve over $\mathcal{O}$. If X is smooth over $\mathcal{O}$ except for a finite number of nodes in X_F, then we say that X *is weakly semistable*. If X is regular and weakly semistable, we say X *is semistable*.

(2) Let X be a weakly semistable curve over $\mathcal{O}$, and let $x \in X_F \subset X$ be a node. We call the length of the $\mathcal{O}_{X,x}$-module $\Omega^2_{X/\mathcal{O},x}$, the *index* of x.

DEFINITION B.7. Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let X_K be a proper smooth curve over K.

(1) If there exist a proper smooth curve $X_{\mathcal{O}}$ over $\mathcal{O}$ and an isomorphism $X_K \to X_{\mathcal{O}} \otimes_{\mathcal{O}} K$ over K, we say that X_K has *good reduction*.

(2) If there exist a proper weakly semistable curve $X_{\mathcal{O}}$ and an isomorphism $X_K \to X_{\mathcal{O}} \otimes_{\mathcal{O}} K$ over K, we say that X_K has *semistable reduction*.

Let $X_{\mathbf{Q}}$ be a proper smooth curve over $\mathbf{Q}$. We say that $X_{\mathbf{Q}}$ has good reduction at a prime p, or semistable reduction at p if, letting $\mathcal{O} = \mathbf{Z}_{(p)}$, $X_{\mathbf{Q}}$ has good reduction, or semistable reduction, respectively.

LEMMA B.8. *Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field. A regular curve X over $\mathcal{O}$ is semistable if all of the following conditions hold: The fiber $X_K \to X$ at the generic point is smooth. The closed fiber X_F is reduced, and as* *a Cartier divisor, it is the sum* $X_F = C_1 + C_2$ *of* $C_1, C_2 \subset X$*, where* C_1*,* C_2 *are smooth curve over* F *and the intersection* $C_1 \cap C_2 = C_1 \times_X C_2$ *is étale over* F*.*

PROOF. Let π be a prime element of $\mathcal{O}$. By Proposition A.4, $X - C_1 \cap C_2$ is smooth over $\mathcal{O}$. We show that $x \in C_1 \cap C_2$ is a node of X_F. Since this assertion is étale local on X, we may assume the residue field of x is F. Replacing X by a neighborhood of x, we suppose C_1 is defined by an element s. Then $t = \pi/s$ defines C_2. Define a morphism of $\mathcal{O}$-schemes $X \to \operatorname{Spec} \mathcal{O}[S,T]/(ST - \pi)$ by $S \mapsto s$ and $T \mapsto t$. We show this is étale at x.

It suffices to show that the homomorphism of the completion $A_0 = \mathcal{O}[[S,T]]/(ST - \pi) \to A = \widehat{\mathcal{O}}_{X,x}$ is an isomorphism. Since $\mathfrak{m}_{A_0}/\mathfrak{m}_{A_0}^2 \to \mathfrak{m}_A/\mathfrak{m}_A^2$ is an isomorphism, $A_0 \to A$ is surjective. Since both A_0 and A are two-dimensional regular local rings, $A_0 \to A$ must be an isomorphism. ☐

LEMMA B.9. *Let* $\mathcal{O}$ *be a discrete valuation ring, let* K *be its field of fractions, let* F *be its residue field, and let* π *be a prime element. Let* X *be a weakly semistable curve over* $\mathcal{O}$*, let* x *be a node of* X_F*, and let* e *be its index. If* $\mathcal{O}$ *is complete and* F *is algebraically closed, then the completion of the local ring* $\mathcal{O}_{X,x}$ *is isomorphic over* $\mathcal{O}$ *to* $\mathcal{O}[[S,T]]/(ST - \pi^e)$*.*

PROOF. Let A be the completion of $\mathcal{O}_{X,x}$. We first show there exist an integer $m \geq 1$ and an isomorphism $\mathcal{O}[[S,T]]/(ST - \pi^m) \to A$. Through the isomorphism $F[[S,T]]/(ST) \to A/(\pi)$, we identify $F[[S,T]]/(ST) = A/(\pi)$. One of the following (i) and (ii) holds.

(i) There exist liftings $s, t \in A$ of the images of S and T, an integer $m \geq 1$, and $u \in A^\times$ such that $st = u\pi^m$.

(ii) If liftings $s, t \in A$ of the images of S and T, an integer $m \geq 1$, and $v \in A$ satisfy $st = v\pi^m$, then v is contained in the maximal ideal (π, s, t) of A.

Suppose (i) holds. Let $A_0 = \mathcal{O}[[S,T]]/(ST - \pi^m)$, and define a morphism of $\mathcal{O}$-algebras $A_0 \to A$ by $S \mapsto s' = su^{-1}$ and $T \mapsto t$. Since the morphism of F-algebras $A_0/(\pi) \to A/(\pi)$ is an isomorphism, and A and A_0 are both $\mathcal{O}$-flat, $A_0/(\pi^n) \to A/(\pi^n)$ is an isomorphism by induction on n. Taking the limit, $A_0 \to A$ is an isomorphism. Since $\Omega^2_{X/\mathcal{O},x}$ is isomorphic to $\varprojlim_n \Omega^2_{(A_0/(\pi^n))/(\mathcal{O}/(\pi^n))} \simeq A_0/(S,T) = \mathcal{O}/(\pi^m)$, we have $e = m$.

Next, we show that (ii) cannot hold. We construct a sequence $(s_m, t_m)_{m=1,2,\dots}$ of liftings of the images of S and T to A such that $s_{m+1} \equiv s_m \bmod \pi^m, t_{m+1} \equiv t_m \bmod \pi^m, s_m t_m \in (\pi^m)$ inductively. We take s_1 and t_1 arbitrarily. Suppose we already have up to s_m, t_m. We can write $s_m t_m = \pi^m v_m$, $v_m = a s_m + b t_m + c\pi$ $(a, b, c \in A)$. If we define $s_{m+1} = s_m - \pi^m b$ and $t_{m+1} = t_m - \pi^m a$, then we have $s_{m+1} t_{m+1} = \pi^{m+1}(c + ab\pi^{m-1})$, and the required conditions hold. If we define $s = \lim_{m\to\infty} s_m$ and $t = \lim_{m\to\infty} t_m$, then s and t are the liftings of the images of S and T, respectively, and $st = 0$. If we define a morphism of $\mathcal{O}$-algebras $\mathcal{O}[[S,T]]/(ST) \to A$ by $S \mapsto s$ and $T \mapsto t$, this is an isomorphism as before. However, since X_K is smooth, A_K must be regular, which is a contradiction. ☐

PROPOSITION B.10. *Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field. Let X and Y be normal curves over $\mathcal{O}$, and let $f : X \to Y$ be finite surjective morphism over $\mathcal{O}$.*

(1) *If X is smooth over $\mathcal{O}$, then $X \to Y$ is flat, and Y is also smooth over $\mathcal{O}$.*
(2) *Suppose X is semistable over $\mathcal{O}$, and let C_1, C_2 be Cartier divisors of X smooth over F satisfying the condition*

$$C_1 + C_2 = X_F,\ C_1 \cap C_2 = \{\textit{nodes of } X_F\},$$
$$\textit{and } C_1 = f^{-1}(f(C_1)),\ C_2 = f^{-1}(f(C_2)). \tag{B.1}$$

Then, Y is weakly semistable over $\mathcal{O}$. Let $D_1 = f(C_1)$ and $D_2 = f(C_2)$ be reduced closed subschemes of Y. Then, D_1 and D_2 are smooth curves over F, and we have $D_1 \cup D_2 = Y_F$ and $D_1 \cap D_2 = \{$nodes of $Y_F\}$.

Furthermore, if x is a node of X_F, then $y = f(x)$ is a node of Y_F. Let e_y be the index of y, let F_x and F_y be the residue fields of x and y, let A and B be the completions of the local rings $\mathcal{O}_{Y,y}$ and $\mathcal{O}_{X,x}$, and let L_x and L_y be the fields of fractions of A and B. Then, we have

$$[F_x : F_y] \cdot e_y = [L_x : L_y]. \tag{B.2}$$

PROOF. (1) Let $\mathcal{O}' \supset \mathcal{O}$ be a complete discrete valuation ring which has the same prime element, and whose residue field F' is an algebraic closure of F. We show that $Y_{\mathcal{O}'} = Y \times_{\mathcal{O}} \mathcal{O}'$ is normal. The morphism $X \to Y$ is flat except for a finite number of closed points of the closed fiber of Y. Thus, by Corollary A.14, Y is smooth except for a finite number of closed points of the closed fiber. Hence, $Y_{\mathcal{O}'}$ is also smooth except for a finite number of closed points of the closed fiber. Since the closed fiber Y_F is reduced, so is the closed fiber $Y_{F'}$. Thus, by Lemma A.41, $Y_{\mathcal{O}'}$ is normal. Replacing $\mathcal{O}$ by $\mathcal{O}'$, we may assume $\mathcal{O}$ is complete and F is algebraically closed.

We show $X \to Y$ is flat. Let $x \in X_F$ be a closed point, and let $y = f(x)$. Let A and B be the completions of the local rings $\mathcal{O}_{Y,y}$ and $\mathcal{O}_{X,x}$, respectively. It suffices to show B is flat over A. Let L_y and L_x be the fields of fractions of A and B, respectively, and let $d = [L_x : L_y]$ be the degree of the extension. Then, $A \to B$ is finite flat of degree d except at the maximal ideal. Choose an isomorphism $\mathcal{O}[[t]] \to B$ and identify as $\mathcal{O}[[t]] = B$. Define a morphism of $\mathcal{O}$-algebras $A_0 = \mathcal{O}[[t']] \to A$ by letting $t' = N_{B/A}t$. Since the valuation of t' in $B/(\pi) = F[[t]]$ is d, $B/(\pi, t') = B \otimes_{A_0} F$ equals $F[[t]]/(t^d)$. Thus, $X \to Y$ is flat by Lemma A.43. Since X is smooth over $\mathcal{O}$, it is regular by Proposition A.13(3). Thus, Y is also smooth by Corollary A.14.

(2) As in (1), we may assume $\mathcal{O}$ is complete and F is algebraically closed. Let x be a node of X_F, and let $y = f(x)$. Let $A = \widehat{\mathcal{O}}_{Y,y} \to B = \widehat{\mathcal{O}}_{X,x}$. Let L_y and L_x be fields of fractions of A and B, respectively, and let $d = [L_x : L_y]$. Choose an isomorphism $\mathcal{O}[[s,t]]/(st - \pi) \to B$, and identify $\mathcal{O}[[s,t]]/(st - \pi) = B$. Suppose the inverse image $\widehat{C}_1$ of C_1 by $\operatorname{Spec} B \to X$ is $V(s)$, and the inverse image $\widehat{C}_2$ of C_2 is $V(t)$. Let $s' = N_{B/A}s$, and let $t' = N_{B/A}t$. Since s' and t' belong to the maximal ideal of A and satisfy $s't' = N_{B/A}\pi = \pi^d$, we obtain a homomorphism $A_0 = \mathcal{O}[[s', t']]/(s't' - \pi^d) \to A$. We show this is an isomorphism.

Since s' equals 0 on $\widehat{C}_1$ and we have $f^{-1}(f(C_1)) = C_1$ by assumption, s' is invertible on $\operatorname{Spec} B - \widehat{C}_1$. Thus, there exists $u \in B^\times$ satisfying $s' = us^d$. Similarly, there exists $v \in B^\times$ satisfying $t' = vt^d$, and thus $B \otimes_{A_0} A_0/\mathfrak{m}_{A_0} = B/(s^d, t^d, \pi) = F[[s,t]]/(s^d, t^d, st)$ is a finite-dimensional $F = A_0/\mathfrak{m}_{A_0}$-vector space. Since B and A_0 are complete, B is finitely generated as an A_0-module by Nakayama's lemma. Since A_0 is a two-dimensional integrally closed domain, $A_0 \to B$ is injective. Thus, the only inverse image of (t') by $\operatorname{Spec} B \to \operatorname{Spec} A_0$ is (t), and the degree of the extension $F((s))/F((s'))$ of residue fields is d since $s' = us^d$. If L_0 is the field of fractions of A_0, then L_x is an extension of L_0 of degree d. Therefore, we have $L_y = L_0$, and $A = A_0$. This shows Y is weakly semistable over $\mathcal{O}$, and the remaining assertions have also been shown. ☐

COROLLARY B.11. *Let $\mathcal{O}$ be a discrete valuation ring, and let X be a curve over $\mathcal{O}$. Suppose an action of a finite group G on X over $\mathcal{O}$ is given, and suppose the quotient $Y = X/G$ exists. Furthermore, if x is the generic point of an irreducible component of X_F and η_x is the generic point of the irreducible component of X containing x, then suppose the inertia groups I_x and I_{η_x} are the same.*

(1) *If X is smooth over $\mathcal{O}$, then so is Y, and we have $Y_F = X_F/G$.*
(2) *Suppose X is semistable over $\mathcal{O}$, and let C_1 and C_2 be smooth Cartier divisors of X over F stable under the G-action satisfying condition* (B.1).

Then Y is also weakly semistable over $\mathcal{O}$, and if $D_1 = f(C_1)$ and $D_2 = f(C_2)$ are reduced closed subschemes, then we have $D_1 = C_1/G$ and $D_2 = C_2/G$.

Moreover, if x is a node of X_F and η_x is the generic point of an irreducible component of x, then the index e_y of the node $y = f(x)$ equals the index $[I_x : I_{\eta_x}]$.

PROOF. (1) By Proposition B.10(1), Y is smooth over $\mathcal{O}$. We show $X_F/G \to Y_F$ is an isomorphism. Since both curves are normal over F, it suffices to show that the residue fields at the generic points of irreducible components are isomorphic. Let x be the generic point of an irreducible component of X_F, and let $y = f(x) \in Y_F$ be its image. Let L_x be the field of fractions of the completion of $\mathcal{O}_{X,x}$, and let L_y be the field of fractions of the completion of $\mathcal{O}_{Y,y}$. Then, L_x is a Galois extension of L_y, and its inertia group is I_x/I_{η_x}. Thus, by assumption, L_x is an unramified extension of L_y. Hence, the residue field $\kappa(x')$ of the image x' in X_F/G of x is equal to $\kappa(y)$, and $X_F/G \to Y_F$ is an isomorphism.

(2) By Proposition B.10(2), Y is weakly semistable over $\mathcal{O}$, and by Corollary B.11(1), the closed immersions $C_1 \to Y$ and $C_2 \to Y$ induce closed immersions $C_1/G \to Y$ and $C_2/G \to Y$ except at nodes. Moreover, by Proposition B.10(2), they define closed immersions at nodes.

Let x be a node, and let $y = f(x)$ be its image. Let L_x be the field of fractions of the completion of $\mathcal{O}_{X,x}$ and let L_y be the field of fractions of the completion of $\mathcal{O}_{Y,y}$. Then L_x is a Galois extension of L_y, and its inertia group is I_x/I_{η_x}. Thus, by Proposition B.10(2), we have $e_x = [I_x : I_{\eta_x}]$. ☐

B.3. Dual chain complex of curves over a discrete valuation ring

Let $\mathcal{O}$ be a discrete valuation ring, and let F be its residue field. Let X be a proper curve over $\mathcal{O}$, and let $\Gamma = [\Gamma_1 \to \Gamma_0]$ be the dual chain complex of X_F. If X is regular, we define a symmetric bilinear form $(\ ,\ )_0 : \Gamma_0 \times \Gamma_0 \to \mathbf{Z}$, and if X is semistable, we define a symmetric bilinear form $(\ ,\ )_1 : \Gamma_1 \times \Gamma_1 \to \mathbf{Z}$.

Let X be a proper flat regular curve over $\mathcal{O}$. For irreducible components C_1 and C_2 of X_F, we define the intersection product $(C_1, C_2)_X$ by $(C_1, C_2)_X = \deg \mathcal{O}_X(C_1)|_{C_2}$. If $C_1 \neq C_2$, it is equal to $\dim_F \Gamma(X, \mathcal{O}_{C_1} \otimes_{\mathcal{O}_X} \mathcal{O}_{C_2})$ and satisfies $(C_1, C_2)_X = (C_2, C_1)_X$. Let $Z_1(X_F)$ be the free $\mathbf{Z}$-module generated by the irreducible components of X_F. Then, the intersection pairing defines a symmetric bilinear form $(\ ,\ )_X : Z^1(X_F) \times Z^1(X_F) \to \mathbf{Z}$. Since the divisor X_F is a principal divisor, $(X_F,\ )$ is the 0-mapping.

LEMMA B.12. *If X_F is connected, then the kernel of the symmetric bilinear form $(\ ,\ )_X$ is generated over $\mathbf{Q}$ by X_F.*

Let F be a perfect field, and let $\Gamma = [\Gamma \to \Gamma_0]$ be the dual chain complex of X_F. Let $\mathcal{O}'$ be the completion of the maximal unramified extension of the completion of $\mathcal{O}$. $\mathcal{O}'$ is a complete discrete valuation ring, and its residue field is an algebraic closure $\overline{F}$ of F. Then, $X_{\mathcal{O}'} = X \times_{\mathcal{O}} \mathcal{O}'$ is a proper regular curve over $\mathcal{O}'$, and we have $X_{\mathcal{O}'} \times_{\mathcal{O}'} F = X_{\overline{F}}$ and $\Gamma_0 = Z_1(X_{\overline{F}})$. Define a symmetric bilinear form

$$(\ ,\ )_0 : \Gamma_0 \times \Gamma_0 \longrightarrow \mathbf{Z} \tag{B.3}$$

by the intersection pairing of $X_{\mathcal{O}'}$. If $X_{\overline{F}}$ is connected, then, by Lemma B.12, the kernel of the bilinear form $(\ ,\ )_0$ is generated by $X_{\overline{F}}$ over $\mathbf{Q}$.

Define a linear mapping

$$\alpha_0 : \Gamma_0 \longrightarrow \Gamma_0^\vee = \mathrm{Hom}(\Gamma_0, \mathbf{Z}) \tag{B.4}$$

by $\alpha_0([C])([C']) = (C, C')_0$, and define a linear mapping

$$\beta : \Gamma_0^\vee \longrightarrow \mathbf{Z} \tag{B.5}$$

as the dual of the linear mapping $\beta^\vee : \mathbf{Z} \to \Gamma_0$ defined by $\beta^\vee(1) = [X_{\bar{F}}] = \sum_C e_C[C]$.

COROLLARY B.13. *Let $\mathcal{O}$ be a discrete valuation ring, and suppose its residue field F is perfect. Let X be a proper regular curve over*

$\mathcal{O}$, and let $\Gamma = [\Gamma_1 \to \Gamma_0]$ be the dual chain complex of X_F. Then, the composition $\beta \circ \alpha_0 : \Gamma_0 \to \Gamma_0^\vee \to \mathbf{Z}$ is the 0-mapping. Moreover, if the geometric fiber $X_{\overline{F}}$ is connected, $\operatorname{Ker}\beta/\operatorname{Im}\alpha_0$ *has finite order.*

PROOF. Since $(X_{\overline{F}},\ \ )_0$ is the 0-mapping, we have $\beta \circ \alpha_0 = 0$. By Lemma B.12, if $X_{\overline{F}}$ is connected, the kernel of the bilinear form $(\ ,\ )_0$ is generated by $X_{\overline{F}}$ over $\mathbf{Q}$. Thus, $\operatorname{Ker}\beta/\operatorname{Im}\alpha_0$ is a finite abelian group. ☐

Let $\mathcal{O}$ be a discrete valuation ring, and let $X_{\mathcal{O}}$ be a proper weakly semistable curve over $\mathcal{O}$. Let $\Gamma = [\Gamma_1 \to \Gamma_0]$ be the dual chain complex of the closed fiber X_F. We use the notation of Definition B.5. For each $x \in \Sigma(\overline{F})$, let x_1, x_2 be the inverse images in $\overline{\Sigma}(\overline{F})$, and define $f_x = [x_1] - [x_2]$. Then, f_x, $x \in \Sigma(\overline{F})$ is a basis of the free $\mathbf{Z}$-module Γ_1. Define a symmetric bilinear form

$$(\ ,\ )_1 : \Gamma_1 \times \Gamma_1 \longrightarrow \mathbf{Z} \tag{B.6}$$

by defining (f_x, f_x) to be the index e_x and letting $(f_x, f_{x'}) = 0$ if $x \neq x'$. This does not depend on the numbering of x_1 and x_2. Define the linear mapping

$$\alpha_1 : \Gamma_1 \longrightarrow \Gamma_1^\vee = \operatorname{Hom}(\Gamma_1, \mathbf{Z}) \tag{B.7}$$

by $\alpha_1(f_x)(f_{x'}) = (f_x, f_{x'})_1$. If $\Gamma^\vee = [\Gamma_0^\vee \to \Gamma_1^\vee]$ is the dual complex of Γ, then $\alpha : \Gamma_1 \to \Gamma_1^\vee$ induces

$$\bar{\alpha}_1 : H_1(\Gamma) = \operatorname{Ker}(\Gamma_1 \to \Gamma_0) \longrightarrow H^1(\Gamma^\vee) = \operatorname{Coker}(\Gamma_0^\vee \to \Gamma_1^\vee). \tag{B.8}$$

If X is weakly semistable, a *minimal resolution of singularities* X' is constructed as follows. Let x be a node of X_F, and let e be its index. Suppose $e \geq 2$, and let X_1 be the blow-up of X at x. If $e = 2$, the exceptional divisor E of X_1 is a smooth conic over x, and X_1 is semistable on a neighborhood of E. If $e \geq 3$, the exceptional curve E is a singular conic and it is smooth over x except at its unique node x_1, and the residue field of x_1 equals that of x. X_1 is weakly semistable, and it is semistable on a neighborhood of E except possibly at x_1, where the index equals $e - 2$. For each node x in X, repeat this procedure $[\frac{e_x}{2}]$ times, and we obtain the minimal resolution of singularities X' of X.

Let $\Gamma' = [\Gamma_1' \to \Gamma_0']$ be the dual complex of the closed fiber X_F' of the minimal resolution of singularities X'. We define a natural morphism $\Gamma \to \Gamma'$ of complexes. We use the notation in Definition B.5. For the minimal resolution of singularities X', let $\overline{X}'_F$ be the normalization of X_F', and define $P' = \operatorname{Spec}\Gamma(\overline{X}'_F, \mathcal{O})$, $\Sigma' = \{\text{nodes of } X_F'\}$, etc. Since the natural morphism $X' \to X$ is an isomorphism outside the nodes of X_F, it induces an open immersion $P \to P'$. Define $\Gamma_0 \to \Gamma'_0$ to be $P \to P'$. The natural morphism $X' \to X$ induces $\Sigma' \to \Sigma$, and for each $x \in \Sigma(\overline{F})$, the number of elements of its inverse image in $\Sigma(\overline{F})$ is the index e_x. For $x \in \Sigma(\overline{F})$, let x_1 and x_2 be its inverse images in $\overline{\Sigma}(\overline{F})$. Let $x'_1, \dots, x'_{e_x}$ be the inverse image of x in $\Sigma'(\overline{F})$, and we choose $x'_{i,1}$, $x'_{i,2}$ to be the inverse images of x'_i, $i = 1, \dots, e_x$, in $\overline{\Sigma}'(\overline{F})$ such that x_1 and $x_{1,1}$, x_2 and $x_{e_x,2}$, and $x_{i,2}$ and $x_{(i+1),1}$ for $1 \leq i < e_x$ are contained pairwise in the same connected component of the normalization $\overline{X}'_{\overline{F}}$. Then, we define homomorphism $\Gamma_1 \to \Gamma'_1$ by letting the image of $([x_1] - [x_2]) \in \Gamma_1$ be $\sum_{i=1}^{e_x}([x_{i,1}] - [x_{i,2}]) \in \Gamma'_1$. The homomorphisms $\Gamma_0 \to \Gamma'_0$ and $\Gamma_1 \to \Gamma'_1$ define a morphism of chain complexes

$$\Gamma \longrightarrow \Gamma'. \tag{B.9}$$

The morphism $\Gamma \to \Gamma'$ induces homomorphisms of homology groups $H_0(\Gamma) \to H_0(\Gamma')$, $H_1(\Gamma) \to H_1(\Gamma')$. The symmetric bilinear form $(\ ,\ ) : \Gamma'_1 \times \Gamma'_1 \to \mathbf{Z}$ induces a symmetric bilinear form $(\ ,\ )_1 : \Gamma_1 \times \Gamma_1 \to Z$ through the linear mapping $\Gamma_1 \to \Gamma'_1$. Thus, $\alpha_1 : \Gamma_1 \to \Gamma_1^\vee$ is obtained as the composition of $\alpha_1 : \Gamma'_1 \to \Gamma'^\vee_1$ with $\Gamma_1 \to \Gamma'_1$ and its dual.

PROPOSITION B.14. *Let $\mathcal{O}$ be a discrete valuation ring, and let X be a proper weakly semistable curve over $\mathcal{O}$. Let $\Gamma = [\Gamma_1 \to \Gamma_0]$ be the dual chain complex of X_F.*

(1) *If X' is the minimal resolution of singularities of X, then the homomorphisms $H_0(\Gamma) \to H_0(\Gamma')$ and $H_1(\Gamma) \to H_1(\Gamma')$ induced by the morphism of chain complexes $\Gamma \to \Gamma'$ in* (B.9) *are isomorphisms.*
(2) *Suppose X is semistable, and let $\bar{\alpha}_1 : H_1(\Gamma) \to H^1(\Gamma^\vee)$ be the linear mapping* (B.8). *Then, we have a natural homomorphism*

$$\begin{aligned} \operatorname{Coker}(\bar{\alpha}_1 : H_1(\Gamma) \to H^1(\Gamma^\vee)) \\ \longrightarrow \operatorname{Ker}(\beta : \Gamma_0^\vee \to \mathbf{Z}) / \operatorname{Im}(\alpha_0 : \Gamma_0 \to \Gamma_0^\vee). \end{aligned} \tag{B.10}$$

PROOF. (1) This is easily verified.

(2) Under the notation in Definition B.5, Γ_0 is a free $\mathbf{Z}$-module generated by $P(\overline{F})$. Sending a basis $P(\overline{F})$ of Γ_0 to its dual basis, we define an isomorphism $\gamma_0 : \Gamma_0 \to \Gamma_0^\vee$. Since $X_{\overline{F}}$ is reduced, the composition $\beta' = \beta \circ \gamma_0 : \Gamma_0 \to \mathbf{Z}$ sends each element of $P(\overline{F})$ to 1. The

composition $\beta' \circ d : \Gamma_1 \to \Gamma_0 \to \mathbf{Z}$ equals 0. Since $X_{\overline{F}}$ is connected, β' induces an isomorphism $\operatorname{Coker} d = H_0(\Gamma) \to \mathbf{Z}$.

Since X is semistable, $\alpha_1 : \Gamma_1 \to \Gamma_1^\vee$ is an isomorphism. Define $\delta_0 : \Gamma_0^\vee \to \Gamma_0$ to be the composition

$$\Gamma_0^\vee \xrightarrow{d^\vee} \Gamma_1^\vee \xrightarrow{\alpha_1^{-1}} \Gamma_1 \xrightarrow{d} \Gamma_0.$$

Identify Γ_1 and $\Gamma_1^\vee$ through the isomorphism $\alpha_1 : \Gamma_1 \to \Gamma_1^\vee$, and regard $\delta_0 : \Gamma_0^\vee \to \operatorname{Ker}\beta'$ as the composition of $d^\vee : \Gamma_0^\vee \to \Gamma_1^\vee$ and $d : \Gamma_1 \to \operatorname{Ker}\beta'$. Then, we obtain an exact sequence

$$\text{(B.11)} \qquad \operatorname{Ker} d \xrightarrow{\bar{\alpha}_1} \operatorname{Coker} d^\vee \xrightarrow{d\circ\alpha_1^{-1}} \operatorname{Ker}\beta' / \operatorname{Im}\delta_0 \longrightarrow \operatorname{Ker}\beta' / \operatorname{Im} d.$$

Since we have $\operatorname{Ker} d = H_1(\Gamma)$, $\operatorname{Coker} d^\vee = H^1(\Gamma^\vee)$, and $\operatorname{Ker}\beta' / \operatorname{Im} d = 0$, (B.11) gives an isomorphism

$$\text{(B.12)} \qquad \operatorname{Coker}(\bar{\alpha}_1 : H_1(\Gamma) \to H^1(\Gamma^\vee)) \\ \longrightarrow \operatorname{Ker}(\beta' : \Gamma_0 \to \mathbf{Z}) / \operatorname{Im}(\delta_0 : \Gamma_0^* \to \Gamma_0).$$

By the isomorphism (B.12), it suffices to show that the diagram

$$\begin{tikzcd}
\Gamma_0 \arrow[r, "\alpha_0"] \arrow[d, "-\gamma_0"'] & \Gamma_0^\vee \arrow[r, "\beta"] \arrow[d, "\gamma_0^{-1}"'] & \mathbf{Z} \arrow[d, equal] \\
\Gamma_0^\vee \arrow[r, "\delta_0"] & \Gamma_0 \arrow[r, "\beta'"] & \mathbf{Z}
\end{tikzcd}$$

commutes. The right square commutes by the definition of β'. We show that the left square commutes. Let D be an irreducible component of $X_{\overline{F}}$. It suffices to show that $-\delta_0 \circ \gamma_0(D) = -d \circ \alpha_1^{-1} \circ d^\vee \circ \gamma_0(D)$ is equal to $\gamma_0^{-1} \circ \alpha_0(D) = \sum_{D'} (D, D')_0 \cdot D'$.

Let $\Sigma_D = \bigcup_{D' \neq D} (D \cap D') \subset \Sigma(\bar{F})$ be the union of the intersections of D and the other irreducible components than D. For each $x \in \Sigma_D$, number the inverse images x_1, x_2 in $\overline{\Sigma}(\overline{F})$ so that $x_1 \in D$. Then, we have

$$\alpha_1^{-1} \circ d^\vee \circ \gamma_0(D) = \sum_{x \in \Sigma_D} ([x_1] - [x_2]).$$

Thus, we have $-d \circ \alpha_1^{-1} \circ d^\vee \circ \gamma_0(D) = -(\sharp\Sigma_D) \cdot D + \sum_{D' \neq D} (D, D')_0 \cdot D'$. Since $(X_{\bar{F}}, D)_0 = 0$, we have $(D, D)_0 = -\sharp\Sigma_D$. This shows the left square is commutative. □

APPENDIX C

Finite commutative group scheme over $\mathbf{Z}_p$

C.1. Finite flat commutative group scheme over $\mathbf{F}_p$

First, we give a description of the category of finite flat commutative group schemes.

THEOREM C.1. *Let p be a prime, and let $n \geq 1$ be an integer. Let G be a finite $\mathbf{Z}/p^n\mathbf{Z}$-module scheme over $\mathbf{F}_p$.*

(1) *There is an equivalence of abelian categories*

$$D : (\textit{finite } \mathbf{Z}/p^n\mathbf{Z}\textit{-module schemes over } \mathbf{F}_p) \\ \to (\textit{finite } \mathbf{Z}/p^n\mathbf{Z}[F,V]/(FV-p)\textit{-module}).$$

(2) *G is étale over $\mathbf{F}_p$ if and only if $F : G \to G$ is an isomorphism and if and only if $F : D(G) \to D(G)$ is an isomorphism. If G is étale, $D(G)$ is the invariant subgroup $(G(\bar{\mathbf{F}}_p) \otimes \mathbf{Z}_p^{\mathrm{ur}})^{G_{\mathbf{F}_p}}$ with respect to the diagonal action of the absolute Galois group $G_{\mathbf{F}_p}$, and the action of F on $D(G) = (G(\bar{\mathbf{F}}_p) \otimes \mathbf{Z}_p^{\mathrm{ur}})^{G_{\mathbf{F}_p}}$ is the restriction of $\varphi_p \otimes 1$*

(3) *If $G^\vee$ is the Cartier dual of G, $D(G^\vee) = \mathrm{Hom}(D(G), \mathbf{Q}_p/\mathbf{Z}_p)$, and $F = V^\vee$, $V = F^\vee$.*

(4) *Let A be an abelian variety over $\mathbf{F}_p$ of dimension g. Then, the $\mathbf{Z}/p^n\mathbf{Z}[F,V]$-module $D(A[p^n])$ is a free $\mathbf{Z}/p^n\mathbf{Z}$-module of rank $2g$. $D(A) = \varprojlim_n D(A[p^n]) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a $\mathbf{Q}_p$-vector space of dimension $2g$. For an endomorphism $f : A \to A$, we have $\deg f = \det(f : D(A))$.*

We omit the proof. $D(G)$ is what is usually called the contravariant *Dieudonné module* $D^\vee(G^\vee)$ of the Cartier dual $G^\vee$. The Frobenius endomorphism F_G of G induces its transpose $V_{G^\vee}$ on $G^\vee$, and thus it acts on $D(G) = D^\vee(G^\vee)$ as $D^\vee(V_{G^\vee})$. In this book we agree on writing F instead of $(F_G)_* = D^\vee(V_{G^\vee})$. If R is a commutative ring and G has a structure of R-module, so does $D(G)$.

If $G = \mathbf{Z}/p^n\mathbf{Z}$, we have $D(G) = \mathbf{Z}/p^n\mathbf{Z}$ and $F = 1$, $V = p$. If $G = \mu_{p^n}$, we have $D(G) = \mathbf{Z}/p^n\mathbf{Z}$ and $F = p$, $V = 1$.

Theorem C.1 is generalized to a general perfect field k of characteristic $p > 0$. Let $W_n(k)$ be the ring of Witt vectors of length n with k coefficients, and let $F : W_n(k) \to W_n(k)$ be the Frobenius endomorphism. Define a noncommutative $W_n(k)$-algebra $W_n(k)\langle F, V\rangle$ generated by F and V by the relations $FV = VF = p$, $Fa = F(a)F$, $aV = VF(a)$ $(a \in W_n(k))$. With this notation we have the following.

THEOREM C.2. *Let p be a prime, and let $n \geq 1$ be an integer. If k is a perfect field of characteristic p, we have an equivalence of abelian categories*

$$D : \left(\begin{array}{l}\textit{finite } \mathbf{Z}/p^n\mathbf{Z}\textit{-module}\\ \textit{schemes over } k\end{array}\right) \to \left(\begin{array}{l}W_n(k)\langle F, V\rangle\textit{-modules of finite}\\ \textit{length as } W_n(k)\textit{-module}\end{array}\right).$$

If k' is a finite extension of k, the following diagram commutes:

$$\begin{tikzcd}
\left(\begin{array}{l}\textit{finite } \mathbf{Z}/p^n\mathbf{Z}\textit{-module}\\ \textit{schemes over } k\end{array}\right) \arrow[r, "D"] \arrow[d, "\otimes_k k'"'] & \left(\begin{array}{l}W_n(k)\langle F, V\rangle\textit{-modules of finite}\\ \textit{length as } W_n(k)\textit{-module}\end{array}\right) \arrow[d, "\otimes_{W_n(k)} W_n(k')"] \\
\left(\begin{array}{l}\textit{finite } \mathbf{Z}/p^n\mathbf{Z}\textit{-module}\\ \textit{schemes over } k'\end{array}\right) \arrow[r, "D"] & \left(\begin{array}{l}W_n(k')\langle F, V\rangle\textit{-modules of finite}\\ \textit{length as } W_n(k')\textit{-module}\end{array}\right)
\end{tikzcd}.$$

C.2. Finite flat commutative group scheme over $\mathbf{Z}_p$

Finite flat commutative group schemes over $\mathbf{Z}_p$ can be described by the following linear algebraic objects.

DEFINITION C.3. Let p be a prime, and let $n \geq 1$ be an integer.

(1) A $\mathbf{Z}/p^n\mathbf{Z}$-module M is a *filtered φ-module* if it is endowed with a submodule M' and linear mappings $\varphi' : M' \to M$ and $\varphi : M \to M$ satisfying $\varphi|_{M'} = p\varphi'$.

(2) A finite filtered φ-module M is *strongly divisible* if $M = \varphi(M) + \varphi'(M')$.

(3) Let M, N be filtered φ-R-modules. An R-linear mapping $f : M \to N$ is a morphism of filtered φ-R-modules if $f(M') \subset N'$, $\varphi \circ f = f \circ \varphi$ and $\varphi' \circ f|_{M'} = f \circ \varphi'$.

(4) A strongly divisible finite filtered φ-module (M, M') is *étale* if $M = M'$. If $M' = 0$, the strongly divisible filtered φ-module (M, M') is said to be *multiplicative*.

LEMMA C.4. *A finite filtered φ-module M is strongly divisible if and only if*

$$0 \longrightarrow M' \xrightarrow{(p,-\mathrm{can})} M' \oplus M \xrightarrow{(\varphi',\varphi)} M \longrightarrow 0 \tag{C.1}$$

is exact.

PROOF. The composition $M' \to M' \oplus M \to M$ is the 0-mapping. By Definition C.3(2), M is strongly divisible if and only if $M' \oplus M \to M$ is surjective. The assertion is now clear by counting the number of elements. □

COROLLARY C.5. (1) *The category of finite strongly divisible filtered φ-modules is an abelian category.*

(2) *If M is a finite strongly divisible filtered φ-module, there exists a linear mapping $F : M \to M$ satisfying $F \circ \varphi = p$ and $F \circ \varphi' = \mathrm{id}_{M'}$.*

(3) *Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbf{Q}_p$. Let $n \geq 1$ be an integer, and let $R = \mathcal{O}/\mathfrak{m}_{\mathcal{O}}^n$. If (M, M') is a finite strongly divisible filtered φ-R-module, M' is a direct summand of M as an R-module.*

(4) *A strongly divisible filtered φ-module (M, M') is étale if and only if $F : M \to M$ is an isomorphism.*

PROOF. (1) Clear from Lemma C.4.

(2) We have $M = \mathrm{Coker}\big((p, -\mathrm{can}) : M' \to M' \oplus M\big)$ from the exact sequence (C.1). The assertion follows immediately from this.

(3) Let F be the residue field of $\mathcal{O}$. The exact sequence (C.1) remains exact after tensoring $\otimes_{\mathcal{O}} F$. Thus, $M' \to M$ is injective after tensoring $\otimes_{\mathcal{O}} F$.

(4) If F is an isomorphism, we have $\varphi = p \circ F^{-1}$, and thus $M = \varphi(M) + \varphi'(M') \subset pM + \varphi'(M')$. Thus, by Nakayama's lemma, $\varphi' : M' \to M$ is surjective and we have $M = M'$. The converse is clear. □

By Corollary C.5(2), an additive functor

$$\begin{aligned}&(\text{finite strongly divisible filtered } \varphi\text{-}\mathbf{Z}/p^n\mathbf{Z}\text{-module})\\ &\qquad\qquad\longrightarrow (\text{finite } \mathbf{Z}/p^n\mathbf{Z}[F, V]/(FV - p)\text{-module})\end{aligned}$$

is defined by letting $V = \varphi$.

THEOREM C.6. *Let p be an odd prime, and let $n \geq 1$ be an integer.*

(1) *There is an equivalence of abelian categories*

(C.2)

$$D : \begin{pmatrix} \text{finite flat } \mathbf{Z}/p^n\mathbf{Z}\text{-module} \\ \text{schemes over } \mathbf{Z}_p \end{pmatrix} \to \begin{pmatrix} \text{finite strongly divisible} \\ \text{filtered } \varphi\text{-}\mathbf{Z}/p^n\mathbf{Z}\text{-module} \end{pmatrix}.$$

The diagram

$$\begin{tikzcd}
\begin{pmatrix} \text{finite flat } \mathbf{Z}/p^n\mathbf{Z}\text{-module} \\ \text{schemes over } \mathbf{Z}_p \end{pmatrix} \arrow[r, "D"] \arrow[d, "\otimes_{\mathbf{Z}_p}\mathbf{F}_p"'] & \begin{pmatrix} \text{finite strongly divisible} \\ \text{filtered } \varphi\text{-}\mathbf{Z}/p^n\mathbf{Z}\text{-module} \end{pmatrix} \arrow[d] \\
\begin{pmatrix} \text{finite flat } \mathbf{Z}/p^n\mathbf{Z}\text{-module} \\ \text{schemes over } \mathbf{F}_p \end{pmatrix} \arrow[r, "D"] & \begin{pmatrix} \text{finite } \mathbf{Z}/p^n\mathbf{Z}[F,V]/(FV-p)\text{-} \\ \text{module} \end{pmatrix}
\end{tikzcd}$$

is commutative.

(2) *For a finite flat $\mathbf{Z}/p^n\mathbf{Z}$-module scheme G over $\mathbf{Z}_p$, G is étale if and only if the corresponding strongly divisible filtered φ-module $D(G)$ is étale. G is multiplicative if and only if $D(G)$ is multiplicative.*

(3) *Let A be an abelian scheme over $\mathbf{Z}_p$ of relative dimension g, and let $D(A) = \varprojlim_n D(A[p^n]) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Then, the subspace $D(A)' = \varprojlim_n D(A[p^n])' \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \subset D(A)$ is a $\mathbf{Q}_p$-vector space of dimension g, and there exist natural isomorphisms of $(\operatorname{End} A) \otimes_{\mathbf{Q}} \mathbf{Q}_p$-modules $D(A)' \to \Gamma(A_{\mathbf{Q}_p}, \Omega^1_{A_{\mathbf{Q}_p}/\mathbf{Q}_p})$ and $D(A)/D(A)' \to \operatorname{Hom}(\Gamma(A_{\mathbf{Q}_p}, \Omega^1_{A_{\mathbf{Q}_p}/\mathbf{Q}_p}), \mathbf{Q}_p)$.*

We do not prove this theorem either. If $G = \mathbf{Z}/p^n\mathbf{Z}$, we have $D(G) = D(G)' = \mathbf{Z}/p^n\mathbf{Z}$ and $\varphi = p$, $\varphi' = 1$. If $G = \mu_{p^n}$, we have $D(G) = \mathbf{Z}/p^n\mathbf{Z}, D(G)' = 0$ and $\varphi = 1$. If R is a commutative ring and G has a structure of R-module, so is $D(G)$.

Let V be a good p-adic representation of $G_{\mathbf{Q}_p}$. A filtered $\mathbf{Q}_p[F]$-module $D(V)$ is defined as follows. Let T be a $G_{\mathbf{Q}_p}$-stable $\mathbf{Z}_p$-lattice in V. For an integer $n \geq 1$, the finite flat commutative group scheme G_n defined by the Galois representation T/p^nT may be extended uniquely to a finite flat commutative group scheme $G_{n,\mathbf{Z}_p}$ over $\mathbf{Z}_p$. Thus, by Theorem C.6, strongly divisible filtered modules $D(G_{n,\mathbf{Z}_p})$ are defined, and these form a inverse system. $D(V) = \varprojlim_n D(G_{n,\mathbf{Z}_p}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is a filtered $\mathbf{Q}_p$-φ-module, and it does not depend on the choice of the $\mathbf{Z}_p$-lattice T. If we let $F = \varphi^{-1} \circ p$, then $D(V)$ becomes a $\mathbf{Q}_p[F]$-module. This coincides with $\varprojlim_n D(G_{n,\mathbf{F}_p}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Let A be an abelian scheme over $\mathbf{Z}_p$, and define a p-adic representation $V_pA_{\mathbf{Q}_p}$ by $V_pA_{\mathbf{Q}_p} = T_pA_{\mathbf{Q}_p} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where $T_pA_{\mathbf{Q}_p}$ is the Tate module. Then, we have $D(V_pA_{\mathbf{Q}_p}) = D(A)$.

Similarly, for a good mod p-representation V of $G_{\mathbf{Q}_p}$, the strongly divisible filtered $\mathbf{F}_p$-φ-module $D(V)$ and also the $\mathbf{F}_p[F, V]/(FV - p)$-module $D(V)$ are defined.

We give a condition for a good two-dimensional representation of $G_{\mathbf{Q}_p}$ to be ordinary.

PROPOSITION C.7. *Let p be an odd prime, and let G be a finite flat commutative group scheme over $\mathbf{Z}_p$. Let $\overline{G} = G/pG$, and let $D(\overline{G})$ be the corresponding strongly divisible filtered φ-module, let n be the multiplicity of the eigenvalue 0 of $\varphi : D(\overline{G}) \to D(\overline{G})$, and let $h = \dim D(\overline{G})'$.*

(1) *The following conditions are equivalent.*
    (i) *There exists a multiplicative closed subgroup scheme H of G such that G/H is étale.*
    (ii) $n = h$.
(2) *Suppose the conditions in (1) hold. Then, $D(H)$ is the maximal submodule of $D(G)$ such that the restriction of φ is an isomorphism, and $D(G)/D(H)$ is the maximal quotient module such that φ induces the 0 homomorphism.*

PROOF. (1). (i) $\Rightarrow$ (ii) It suffices to show it assuming $G = \overline{G}$ and $\overline{G}$ is either étale or multiplicative. If $\overline{G}$ is étale, we have $n = h = \dim D(\overline{G})$ by Theorem C.6(2) and Corollary C.5(4). Similarly, if $\overline{G}$ is multiplicative, we have $n = h = 0$.

(ii) $\Rightarrow$ (i) The subring $\mathbf{Z}_p[\varphi] \subset \operatorname{End} D(G)$ is the direct product of the part φ is invertible and the part φ is nilpotent. Thus, $D(G)$ also decomposes to the direct sum of the part $D(G)^o$ in which φ is invertible and the part φ is nilpotent. We show $D(G)^o \cap D(G)' = 0$. Assume $0 \neq x \in D(G)^o \cap D(G)'$, and we deduce a contradiction. We may assume $px = 0$. Since $0 \neq x \in D(G)^o$, we have $\varphi(x) \neq 0$. But, since $x \in D(G)'$ and $px = 0$, we have $\varphi(x) = p\varphi'(x) = \varphi'(px) = 0$, which is a contradiction. Hence, the natural mapping $D(G)^o \oplus D(G)' \to D(G)$ is injective.

Since $\dim D(\bar{G}) = \dim D(\bar{G})^o + n$ and $\dim D(\bar{G})' = h$, the injection $D(\bar{G})^o \oplus D(\bar{G})' \to D(\bar{G})$ is an isomorphism if $n = h$. Thus, by Nakayama's lemma, $D(G)^o \oplus D(G)' \to D(G)$ is surjective, and an isomorphism. From this we obtain an exact sequence of strongly divisible filtered φ-modules

$$0 \longrightarrow (D(G)^o, 0) \longrightarrow (D(G), D(G)') \longrightarrow (D(G)', D(G)') \longrightarrow 0.$$

The assertion now follows from Theorem C.6(2).

(2) Clear from the proof of (1) (ii) $\Rightarrow$ (i). ☐

COROLLARY C.8. *Let p be an odd prime, let K be a finite extension of $\mathbf{Q}_p$, and let $\mathcal{O}$ be its ring of integers. Let V be a good representation of $G_{\mathbf{Q}_p}$ on a two-dimensional K-vector space, and let $D = D(V)$ be the corresponding filtered $K[F]$-module. Suppose* $\dim D(V)' = 1$. *Then, for V to be ordinary, it is necessary and sufficient that there exist p-adic units satisfying* $\det(1 - Ft : D) = (1 - \alpha t)(1 - p\beta t)$.

Suppose this condition holds, and let α, β denote the unramified characters of $G_{\mathbf{Q}_p}$ such that the value of φ is α, β, respectively, and χ the p-adic cyclotomic character. Then, V is an extension of α by $\beta \cdot \chi$.

PROOF. It is clear that the condition is necessary. We show it is sufficient. Suppose $\det(1 - Ft : D) = (1 - \alpha t)(1 - p\beta t)$ and α, β are p-adic units. Let $D^o \subset D$ be the eigenspace belonging to the eigenvalue $p\beta$ of F, and $T \subset V$ a $G_{\mathbf{Q}_p}$-stable $\mathcal{O}$-lattice. $D(T)^o = D(T) \cap D^o$ is a free $\mathcal{O}$-module of rank 1, and the action of φ on $D(T)^o$ is the multiplication by $1/\beta$, and its action on $D(T)/D(T)^o$ is the multiplication by p/α.

For an integer $m \geq 1$, let G_m be the finite flat commutative group scheme over $\mathbf{Z}_p$ defined by $G_m(\bar{\mathbf{Q}}_p) = T/p^m T$. Then, n and h in Proposition C.7 are both equal to $[K : \mathbf{Q}_p]$. Thus, by Proposition C.7, there exists a subrepresentation T^o of T such that $D(T^o) = D(T)^o$ and that both T/T^o and $T^o(-1)$ are unramified. Since the action of φ on $D(T/T^o) = D(T)/D(T)^o$ is p/α, the action of F is α, and by Theorem C.1(2), the action of φ_p on T/T^o is also α. Similarly, the action of φ_p on $T^o(-1)$ is multiplication by β. ☐

We give a description of an extension of strongly divisible filtered φ-R-modules. Let R be a finite commutative algebra over $\mathbf{Z}_p$, and let M, N be strongly divisible filtered φ-R-modules. As in §11.1, an exact sequence of strongly divisible filtered φ-R-modules $(E) : 0 \to N \to E \to M \to 0$ is called an *extension* of M by N.

If there is a commutative diagram

$$\begin{tikzcd}
(E) : 0 \arrow[r] & N \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, equal] & 0 \\
(E') : 0 \arrow[r] & N \arrow[r] & E' \arrow[r] & M \arrow[r] & 0,
\end{tikzcd}$$

we say that the extensions (E) and (E') are isomorphic. The set of isomorphism classes $\mathrm{Ext}^{\varphi}_R(M,N)$ has a structure of R-module. By the equivalence of categories (C.2), for finite flat R-module schemes G, H over $\mathbf{Z}_p$, the group $\mathrm{Ext}_R(G,H)$ of isomorphism classes of extensions of G by H is naturally identified with $\mathrm{Ext}^{\varphi}_R(D(G),D(H))$.

For filtered φ-R-modules M, N, define

$$\begin{aligned}
&\mathbf{Hom}_R(M,N) \\
&\qquad = \{(f,g) \in \mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(M',N) \mid f|_{M'} = pg\}, \\
&\mathbf{Hom}_R(M,N)' = \{f \in \mathrm{Hom}_R(M,N) \mid f(M') \subset N'\},
\end{aligned}$$

and define a homomorphism $\delta : \mathbf{Hom}_R(M,N)' \to \mathbf{Hom}_R(M,N)$ by $\delta(f) = (\varphi \circ f - f \circ \varphi, \varphi' \circ f|_{M'} - f \circ \varphi')$. We denote by $\mathrm{Hom}^{\varphi}_R(M,N)$ the set of homomorphisms $M \to N$ of filtered φ-R-modules. For $(f,g) \in \mathbf{Hom}_R(M,N)$, define an extension $E = E_{f,g}$ of M by N by $E = M \oplus N$, $E' = M' \oplus N'$, $\varphi(x,y) = (\varphi(x), \varphi(y) + f(x))$, $\varphi'(x,y) = (\varphi'(x), \varphi'(y) + g(x))$. A homomorphism $\mathbf{Hom}_R(M,N) \to \mathrm{Ext}^{\varphi}_R(M,N)$ is defined by assigning to (f,g) the isomorphism class $E_{f,g}$.

PROPOSITION C.9. *Let p be an odd prime. Let R be a $\mathbf{Z}_p$-algebra. Let G, H be finite flat R-module schemes over $\mathbf{Z}_p$, and let $M = D(G)$, $N = D(H)$ be corresponding strongly divisible filtered φ-R-modules. Then, there exists an exact sequence of R-modules*

$$\text{(C.3)} \quad 0 \to \mathrm{Hom}_R(G,H) \longrightarrow \mathbf{Hom}_R(M,N)' \xrightarrow{\delta} \mathbf{Hom}_R(M,N) \longrightarrow \mathrm{Ext}_R(G,H).$$

Furthermore, if M is a free R-module, then there exists an exact sequence

$$\text{(C.4)} \quad 0 \to \mathrm{Hom}_R(G,H) \longrightarrow \mathbf{Hom}_R(M,N)' \xrightarrow{\delta} \mathbf{Hom}_R(M,N) \longrightarrow \mathrm{Ext}_R(G,H) \to 0.$$

PROOF. First we show the exact sequence (C.3). We identify $\mathrm{Hom}_R(G,H) = \mathrm{Hom}^{\varphi}_R(M,N)$ and $\mathrm{Ext}_R(G,H) = \mathrm{Ext}^{\varphi}_R(M,N)$ by

Theorem C.6(1). It is clear from the definition that $\mathrm{Hom}^{\varphi}_R(M,N)$ is the kernel of $\delta : \mathbf{Hom}_R(M,N)' \to \mathbf{Hom}_R(M,N)$. We show the exactness at $\mathbf{Hom}_R(M,N)$. If for $(f,g) \in \mathbf{Hom}_R(M,N)$, the class of $E_{f,g}$ is 0, we have an isomorphism $E_{f,g} \to E_{0,0}$. Its component $h : M \to N$ gives an element of $\mathbf{Hom}_R(M,N)'$ satisfying $(f,g) = \delta(h)$. Thus, the sequence is exact at $\mathbf{Hom}_R(M,N)$.

We show $\mathbf{Hom}_R(M,N) \to \mathrm{Ext}^{\varphi}_R(M,N)$ is surjective assuming M is a free R-module. Let E be an extension of M by N. Since M' is the direct sum of M, if M is a free R-module, M' is a projective R-module. Thus, there exists a direct sum decomposition $E = M \oplus N$ of R-modules that is an extension of the direct sum decomposition $E' = M' \oplus N'$ as R-modules. The surjectivity of $\mathbf{Hom}_R(M,N) \to \mathrm{Ext}^{\varphi}_R(M,N)$ follows from this and the definition. ☐

COROLLARY C.10. *Let p be an odd prime, and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbf{Q}_p$. Let $n \geq 1$ be an integer, and let $R = \mathcal{O}/\mathfrak{m}^n_{\mathcal{O}}$. Let G, H be finite flat R-module schemes over $\mathbf{Z}_p$, and suppose $G(\overline{\mathbf{Q}}_p)$ is a free R-module. Let M and N be strongly divisible filtered φ-R-module corresponding G and H, respectively. Then, we have*

$$\frac{\sharp\,\mathrm{Ext}_R(G,H)}{\sharp\,\mathrm{Hom}_R(G,H)} = \sharp\,\mathrm{Hom}_R(M', N/N').$$

PROOF. We show M is a free R-modules. By Nakayama's lemma, for M to be a free R-module, it is necessary and sufficient that $\sharp M = \sharp(M/\mathfrak{m}_{\mathcal{O}}M)^n$. Thus, for M to be free, it is necessary and sufficient that $G(\overline{\mathbf{Q}}_p)$ is a free R-module.

By Proposition C.9, the left-hand side equals $\frac{\sharp\,\mathbf{Hom}_R(M,N)}{\sharp\,\mathbf{Hom}'_R(M,N)}$. By Corollary C.5(3), M' is a direct summand of M. Thus, $\mathbf{Hom}_R(M,N)$ and $\mathbf{Hom}_R(M,N)'$ are the kernels of the surjections

$$\mathrm{Hom}_R(M,N) \oplus \mathrm{Hom}_R(M',N) \to \mathrm{Hom}_R(M',N) : (f,g) \mapsto f|_{M'} - pg,$$

$$\mathrm{Hom}_R(M,N) \oplus \mathrm{Hom}_R(M',N') \to \mathrm{Hom}_R(M',N) : (f,g) \mapsto f|_{M'} - g.$$

Therefore, the left-hand side is equal to $\frac{\sharp\,\mathrm{Hom}_R(M',N)}{\sharp\,\mathrm{Hom}'_R(M',N')}$, and equal to the right-hand side. ☐

APPENDIX D

Jacobian of a curve and its Néron model

The group of divisors of degree 0 of Riemann surfaces has the structure of a compact complex torus. For a curve over any field, or more generally, over a scheme, the group of divisors of degree 0 has a natural algebraic geometric structure. We call it the Jacobian of a curve. In Chapter 9, we constructed a Galois representation associated with modular forms using this algebraic structure for the modular curves. For a prime number at which a curve has bad reduction, its Jacobian may not have good reduction. Even for such a prime number, we can still study its properties using the Néron model.

D.1. The divisor class group of a curve

Let X be a proper normal connected curve over a field k. Let K be the function field of X. A formal linear combination of closed points with $\mathbf{Z}$ coefficients is called the *divisor* of X. The free abelian group generated by the closed points of X

$$\text{(D.1)} \qquad \mathrm{Div}(X) = \bigoplus_{x\text{:closed point of } X} \mathbf{Z}\cdot[x]$$

is called the *divisor group*. For a rational function $f \in K^\times$ on X, the divisor of f, noted $\mathrm{div}\, f$, is defined by $\sum_x \mathrm{ord}_x f \cdot [x] \in \mathrm{Div}(X)$. By associating to $f \in K^\times$ the divisor $\mathrm{div}\, f \in \mathrm{Div}(X)$, we obtain a homomorphism of abelian groups $\mathrm{div} : K^\times \to \mathrm{Div}(X)$. An element of the image of this homomorphism is called a *principal divisor*, and the cokernel

$$\text{(D.2)} \qquad \mathrm{Pic}(X) = \mathrm{Div}(X)/\,\mathrm{div}\, K^\times$$

is called the *divisor class group*.

The divisor class group $\mathrm{Pic}(X)$ has the following cohomological expression. Denote by $K^\times$ the constant sheaf on X, and for a closed point x, let $\mathbf{Z}_x$ be the extension to X of the constant sheaf on x.

Since the local ring at each closed point of X is a discrete valuation ring, we obtain an exact sequence of sheaves on X

$$0 \longrightarrow \mathbf{G}_m \longrightarrow K^\times \xrightarrow{\oplus_x \operatorname{ord}_x} \bigoplus_{x:\text{closed point of } X} \mathbf{Z}_x \longrightarrow 0. \tag{D.3}$$

The long exact sequence induced by this yields an isomorphism

$$\operatorname{Pic}(X) \longrightarrow H^1(X, \mathbf{G}_m). \tag{D.4}$$

In what follows we identify $\operatorname{Pic}(X) = H^1(X, \mathbf{G}_m)$ through this isomorphism.

For $D = \sum_x n_x[x]$ in X, we call $\deg D = \sum_x n_x[\kappa(x) : k]$ the degree of the divisor D. Associating to the divisor $D \in \operatorname{Div}(X)$ to its degree $\deg D \in \mathbf{Z}$, we obtain a homomorphism of abelian groups $\deg : \operatorname{Div}(X) \to \mathbf{Z}$. Since the degree of a principal divisor is 0, this induces a homomorphism $\deg : \operatorname{Pic}(X) \to \mathbf{Z}$. Its kernel $\operatorname{Ker}(\deg : \operatorname{Pic}(X) \to \mathbf{Z})$ is denoted by $\operatorname{Pic}^0(X)$, and is called the divisor class group of degree 0.

Let $f : X \to Y$ be a finite flat morphism of proper normal connected curves. Define $f^* : \operatorname{Div}(Y) \to \operatorname{Div}(X)$ by $f^*([y]) = [X \times_Y y] = \sum_{x \mapsto y} e_{x/y}[x]$ for a closed point y in Y. Here, $e_{x/y}$ indicates the ramification index at x. $f^* : \operatorname{Div}(Y) \to \operatorname{Div}(X)$ induces $f^* : \operatorname{Pic}(Y) \to \operatorname{Pic}(X)$ and $f^* : \operatorname{Pic}^0(Y) \to \operatorname{Pic}^0(X)$. $f_* : \operatorname{Div}(X) \to \operatorname{Div}(Y)$ is defined by $f_*([x]) = f_{x/f(x)}[f(x)]$ for a closed point x in X. Here, $f_{x/f(x)}$ indicates the degree of extension $[\kappa(x) : \kappa(f(x))]$ of the residue field. $f_* : \operatorname{Div}(X) \to \operatorname{Div}(Y)$ induces $f_* : \operatorname{Pic}(X) \to \operatorname{Pic}(Y)$ and $f_* : \operatorname{Pic}^0(X) \to \operatorname{Pic}^0(Y)$.

The Jacobian of a curve X is defined as the divisor class group $\operatorname{Pic}^0(X)$ of degree 0 equipped with a geometric structure. In the next section we define the Jacobian of X as the moduli space of the Picard functor. In this section we give an analytic expression of the Jacobian when k is the complex number field.

Let X be a smooth connected curve over $\mathbf{C}$ of genus g, and let X^{an} be the Riemann surface associated with X. Consider the singular chain complex $(C_q(X^{\mathrm{an}}, \mathbf{Z}), d_q)_{q \in \mathbf{Z}}$ of X^{an}. The fact that $H_0(X^{\mathrm{an}}, \mathbf{Z}) = \mathbf{Z}$ implies

$$\begin{aligned} \operatorname{Div}^0(X) &= \operatorname{Ker}(C_0(X^{\mathrm{an}}, \mathbf{Z}) \to H_0(X^{\mathrm{an}}, \mathbf{Z})) \\ &= \operatorname{Im}(C_1(X^{\mathrm{an}}, \mathbf{Z}) \to C_0(X^{\mathrm{an}}, \mathbf{Z})), \end{aligned}$$

and we obtain a surjection $C_1(X^{\mathrm{an}}, \mathbf{Z}) \to \mathrm{Div}^0(X)$. Define a homomorphism

$$C_1(X^{\mathrm{an}}, \mathbf{Z}) \longrightarrow H^0(X, \Omega^1_X)^\vee = \mathrm{Hom}(H^0(X, \Omega^1_X), \mathbf{C}) \tag{D.5}$$

by associating to 1-chain γ the linear form $\omega \mapsto \int_\gamma \omega$. (D.5) induces a homomorphism

$$\mathrm{Div}^0(X) \longrightarrow H^0(X, \Omega^1_X)^\vee / \operatorname{Im} H_1(X^{\mathrm{an}}, \mathbf{Z}). \tag{D.6}$$

The mapping induced by (D.5)

$$H_1(X^{\mathrm{an}}, \mathbf{Z}) \longrightarrow H^0(X, \Omega^1_X)^\vee \tag{D.7}$$

induces an isomorphism of $\mathbf{R}$-vector spaces

$$H_1(X^{\mathrm{an}}, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{R} \longrightarrow H^0(X, \Omega^1_X)^\vee. \tag{D.8}$$

In other words, the free abelian group $H_1(X^{\mathrm{an}}, \mathbf{Z})$ of rank $2g$ is a lattice in the $\mathbf{C}$-vector space $H^0(X, \Omega^1_X)^\vee$ of dimension g. Thus, $H^0(X, \Omega^1_X)^\vee / \operatorname{Im} H_1(X^{\mathrm{an}}, \mathbf{Z})$ is a complex torus of dimension g.

By Abel's theorem, (D.6) induces an isomorphism

$$\mathrm{Pic}^0(X) \to H^0(X, \Omega^1_X)^\vee / \operatorname{Im} H_1(X^{\mathrm{an}}, \mathbf{Z}). \tag{D.9}$$

In this way $\mathrm{Pic}^0(X)$ has a structure of compact complex torus of dimension g.

Let $\mathbf{Z}(1)$ be the constant sheaf $2\pi\sqrt{-1}\mathbf{Z}$ on X^{an}. The trace mapping $H^2(X^{\mathrm{an}}, \mathbf{Z}(1)) \to \mathbf{Z}$ is an isomorphism. By the Poincaré duality, $H^1(X^{\mathrm{an}}, \mathbf{Z}(1))$ is identified with $H_1(X^{\mathrm{an}}, \mathbf{Z})$, the dual of $H^1(X^{\mathrm{an}}, \mathbf{Z})$.

D.2. The Jacobian of a curve

We define the Picard functor, and give an algebraic geometric structure to the divisor class group of degree 0 of a curve.

Let X be a scheme. Denote by $\mathrm{Pic}(X)$ the set of isomorphism classes of invertible sheaves on X. Define the product of the classes of invertible sheaves $\mathcal{L}$ and $\mathcal{L}'$ by $[\mathcal{L}] \cdot [\mathcal{L}'] = [\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}']$. Then, $\mathrm{Pic}(X)$ is a commutative group, called the *Picard group* of X. If X is a normal connected curve over a field k, $\mathrm{Pic}(X)$ coincides with the divisor class group of X.

If $\mathcal{L}$ is an invertible sheaf on X, $\mathcal{I}som_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{L})$ defines a $\mathbf{G}_m$-torsor over X. Thus, we obtain a natural homomorphism

$$\mathrm{Pic}(X) \longrightarrow H^1(X, \mathbf{G}_m). \tag{D.10}$$

Conversely, if a $\mathbf{G}_m$-torsor over X is given, we obtain an invertible sheaf by patching, and thus (D.10) is an isomorphism. In what follows we identify $\mathrm{Pic}(X) = H^1(X, \mathbf{G}_m)$ via (D.10).

Let S be a scheme, and let X be a scheme over S. Define a functor $P_{X/S}$ over S by associating to a scheme T over S the commutative group $\mathrm{Pic}(X \times_S T)$. The definition of the functor $P_{X/S}$ is too naive, and we cannot expect in general that such a functor is representable. So, we give the following definition.

Definition D.1. Let S be a scheme, and let X be a scheme over S. The flat sheafification $P^{\mathfrak{a}}_{X/S}$ of the functor $P_{X/S}$ over S defined by

$$P_{X/S}(T) = \mathrm{Pic}(X \times_S T) \tag{D.11}$$

is called the *Picard functor* and is denoted by $\mathrm{Pic}_{X/S}$. If k is a field and $S = \mathrm{Spec}\, k$, then $\mathrm{Pic}_{X/S}$ is also written as $\mathrm{Pic}_{X/k}$.

For a geometric point $\bar{s}$, the natural map $P_{X/S}(\bar{s}) = \mathrm{Pic}(X_{\bar{s}}) \to \mathrm{Pic}_{X/S}(\bar{s})$ is an isomorphism. If X is a smooth conic over k, the degree mapping defines an isomorphism $\mathrm{Pic}_{X/k}(k) \to \mathbf{Z}$, and the natural map $\mathrm{Pic}(X) \to \mathrm{Pic}_{X/k}(k)$ is injective. If X has a rational point, this mapping is an isomorphism; if not, its image is $2\mathbf{Z}$.

Let S be a scheme, and let $f : X \to Y$ be a morphism of schemes over S. Then, the pullback of an invertible sheaf by f defines a morphism of functors $f^* : \mathrm{Pic}_{Y/S} \to \mathrm{Pic}_{X/S}$. If $f : X \to Y$ is finite flat of finite presentation, the norm of an invertible sheaf defines a morphism of functors $f_* : \mathrm{Pic}_{X/S} \to \mathrm{Pic}_{Y/S}$. If $\mathcal{L}$ is an invertible sheaf on X, the *norm* $N_f\mathcal{L}$ is defined as an invertible sheaf on Y as follows. For a point y in Y, there exists an open neighborhood V and a basis ℓ_V of an $\mathcal{O}_{f^{-1}(V)}$-module $\mathcal{L}|_{f^{-1}(V)}$. $N_f\mathcal{L}$ is an invertible sheaf that has a basis $N(\ell_V)$ over V, and for a change of bases $\ell' = a\ell$ we have $N(\ell') = N_{X/Y}a \cdot N(\ell)$.

Definition D.2. Let S be a scheme, and let X be a proper curve over S.

(1) Let k be a field, and let $S = \mathrm{Spec}\, k$. Let $\overline{X}$ be a normalization of X, and let $X_1, \dots X_n$ be its connected components. Define

$$\mathrm{Pic}^0(X) = \bigcap_{i=1}^{n} \mathrm{Ker}\big(\mathrm{Pic}(X) \to \mathrm{Pic}(X_i) \overset{\deg}{\to} \mathbf{Z}\big). \tag{D.12}$$

A subfunctor $\mathrm{Pic}^0_{X/S}$ of $\mathrm{Pic}_{X/S}$ is defined by

$$(\mathrm{D}.13)\quad \mathrm{Pic}^0_{X/S}(T) = \bigcap_{\substack{\bar{t}:\text{geometric}\\ \text{point of } T}} \left(\begin{array}{l}\text{inverse image of } \mathrm{Pic}_{X/S}(T) \to \\ \mathrm{Pic}_{X/S}(\bar{t}) = \mathrm{Pic}(X_{\bar{t}}) \text{ by } \mathrm{Pic}^0(X_{\bar{t}})\end{array}\right)$$

for a scheme T over S.

The following theorem is fundamental.

THEOREM D.3. *Let S be a scheme, and let $f : X \to S$ be a proper smooth curve over S of genus g such that each geometric fiber is connected.*

(1) *$\mathrm{Pic}^0_{X/S}$ is representable by an abelian scheme $j : J \to S$ over S of relative dimension g.*
(2) *There is a natural isomorphism*

$$(\mathrm{D}.14)\qquad j_*\Omega_{J/S} \to f_*\Omega_{X/S}.$$

(3) *Let $n \geq 1$ be an integer. The Weil pairing defines a bilinear form $J[n] \times J[n] \to \mu_n$ and defines an isomorphism to the Cartier dual*

$$(\mathrm{D}.15)\qquad J[n] \longrightarrow J[n]^\vee.$$

The moduli space J of the functor $\mathrm{Pic}^0_{X/S}$ is call the *Jacobian* of X.

EXAMPLE D.4. Let S be a scheme, and let E be an elliptic curve over S. The morphism of functors $E \to \mathrm{Pic}^0_{E/S}$, defined by associating to a scheme T over S and a section $P : T \to E$ over T the invertible sheaf $\mathcal{O}_{E_T}([P] - [O])$, is an isomorphism. By this isomorphism, the Jacobian of E is identified with E itself.

COROLLARY D.5. *Let k be a field, and let X be a proper smooth curve over k of genus g such that the geometric fiber $X_{\bar{k}}$ is connected.*

(1) *The Jacobian $J = \mathrm{Pic}^0_{X/k}$ is an abelian variety over k of dimension g.*
(2) *There is a natural isomorphism*

$$(\mathrm{D}.16)\qquad \Gamma(J, \Omega_{J/k}) \longrightarrow \Gamma(X, \Omega_{X/k}).$$

(3) *Let $n \geq 1$ be an integer. The Weil pairing defines a bilinear form $J[n] \times J[n] \to \mu_n$ and the isomorphism $J[n] \to J[n]^\vee$ to its Cartier dual.*

The Jacobian of X is sometimes denoted by $\mathrm{Jac}(X)$.

Let $k = \mathbf{C}$. Identify $J[n] = H_1(X^{\mathrm{an}}, \mathbf{Z}/n\mathbf{Z}) = H^1(X^{\mathrm{an}}, \mathbf{Z}/n\mathbf{Z}(1))$. The Weil pairing $J[n] \times J[n] \to \mu_n$ may be identified with the pairing $H_1(X^{\mathrm{an}}, \mathbf{Z}/n\mathbf{Z}) \times H_1(X^{\mathrm{an}}, \mathbf{Z}/n\mathbf{Z}) \to \mathbf{Z}/n\mathbf{Z}(1)$ that is induced by the composition of the cup product $H^1(X^{\mathrm{an}}, \mathbf{Z}(1)) \times H^1(X^{\mathrm{an}}, \mathbf{Z}(1)) \to H^2(X^{\mathrm{an}}, \mathbf{Z}(2))$ and the trace mapping $H^2(X^{\mathrm{an}}, \mathbf{Z}(2)) \to \mathbf{Z}(1)$.

Let $f : X \to Y$ be a finite flat morphism of proper smooth curves over k. The morphisms of functors $f_* : \mathrm{Pic}_{X/k} \to \mathrm{Pic}_{Y/k}$, $f^* : \mathrm{Pic}_{Y/k} \to \mathrm{Pic}_{X/k}$ induce morphisms of Jacobians $f_* : J_X \to J_Y$, $f^* : J_Y \to J_X$.

LEMMA D.6. *Let $f : X \to Y$ be a finite flat morphism of proper smooth curves over k.*

(1) *The kernel of $f^* : J_Y \to J_X$ is finite over k.*
(2) *Let X be a Galois covering of Y, and let G be its Galois group. If ℓ is a prime number invertible in k, $f^* : V_\ell J_Y \to V_\ell J_X$ defines an isomorphism $f^* : V_\ell J_Y \to (V_\ell J_X)^G$ to the G-invariant part $(V_\ell J_X)^G$.*

PROOF. (1) Since $f_* \circ f^* : J_Y \to J_Y$ is the multiplication-by-$[X : Y]$ mapping, $\mathrm{Ker}\, f^*$ is finite.

(2) It is clear from the fact that $f^* \circ f_* : J_X \to J_X$ equals $\sum_{g \in G} g^*$. □

THEOREM D.7. *Let k be a field, and let X be a proper curve over k.*

(1) *The functor $\mathrm{Pic}^0_{X/k}$ is represented by a smooth connected commutative group scheme J over k.*
(2) *Suppose X is smooth. Let $X = \coprod_{i=1}^n X_i$ be the decomposition into connected components, and let $k_i = \Gamma(X_i, \mathcal{O})$ be the field of definition of X_i for $i = 1, \ldots, n$. Then, J is an abelian variety that is isomorphic to the product $\prod_{i=1}^n \mathrm{Res}_{k_i/k} J_i$ of the Weil restrictions to k of the Jacobian $J_i = \mathrm{Pic}^0_{X_i/k_i}$ of X_i over k_i.*
(3) *Suppose X is smooth except for a finite number of ordinary double points. Let $\overline{X}$ be its normalization. Then J is an extension of the Jacobian $\overline{J}$ of $\overline{X}$ by a torus.*
(4) *Assume k is perfect. Let $\overline{X}$ be the normalization of X, and let Γ be the dual chain complex of X. Then, the morphism $J \to \overline{J}$ induced by the natural map $\overline{X} \to X$ gives an isomorphism from the abelian part J^{a} of J*

$$J^{\mathrm{a}} \longrightarrow \overline{J}. \tag{D.17}$$

The character group of the torus part J^{t} *of* J *is naturally isomorphic to* $H_1(\Gamma)$.

D.3. The Néron model of an abelian variety

THEOREM D.8. *Let* $\mathcal{O}$ *be a discrete valuation ring, and let* K *be its field of fractions. Let* A_K *be an abelian variety over* K. *Then, there exists a smooth commutative group scheme* A *over* $\mathcal{O}$ *having the following property: for any smooth scheme* X *over* $\mathcal{O}$, *the restriction mapping*

$$\{\text{morphism } X \to A \text{ of schemes over } \mathcal{O}\} \\ \longrightarrow \{\text{morphism } X_K \to A_K \text{ of schemes over } K\}$$

is an isomorphism.

The smooth commutative group scheme over $\mathcal{O}$ satisfying the condition in Theorem D.8 is unique up to natural isomorphisms.

DEFINITION D.9. Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field. Let A_K be an abelian variety over K. The smooth commutative group scheme A over $\mathcal{O}$ that satisfies the property in Theorem D.8 is called the *Néron model* of A_K.

The open subgroup scheme A^0 of A, which is defined by the conditions $A^0 \otimes_{\mathcal{O}} K = A \otimes_{\mathcal{O}} K$ and that $A^0 \otimes_{\mathcal{O}} F$ is the connected component A^0_F of $A \otimes_{\mathcal{O}} F$ containing the identity element, is called the *connected component* of the Néron model A.

DEFINITION D.10. Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field. Let A_K be an abelian variety over K, and let A be the Néron model of A_K.

(1) If A is an abelian scheme over $\mathcal{O}$, A_K is said to have *good reduction.*

(2) If the connected component A^0_F of the closed fiber A_F of A is an extension of an abelian variety by a torus, A_K is said to have *semistable reduction.*

LEMMA D.11. *Let* $\mathcal{O}$ *be a discrete valuation ring, let* K *be its field of fractions, and let* F *be its residue field. Let* A_K *be an abelian variety over* K *that has good reduction, let* A *be the Néron model of* A_K, *and let* $A_F = A \otimes_{\mathcal{O}} F$ *be its reduction. Let* ℓ *be a prime number different from the characteristic of* F.

(1) *The Tate module* $T_\ell A_K$ *is an unramified representation of* G_K*, and the natural isomorphism* $T_\ell A_K \to T_\ell A_F$ *is compatible with the natural surjection* $G_K \to G_F$*.*

(2) *The natural isomorphism* $\operatorname{End} A_K \to \operatorname{End} A_F$ *is injective, and it is compatible with the natural isomorphism* $T_\ell A_K \to T_\ell A_F$*.*

PROOF. (1) It follows easily from Lemma A.47(1).

(2) It follows easily from Proposition A.51(2). □

PROPOSITION D.12. *Let* $\mathcal{O}$ *be a discrete valuation ring, let* K *be its field of fractions, and let* F *be its residue field. Let* A_K *be an abelian variety over* K*, and let* G *be a finite flat commutative group scheme over* $\mathcal{O}$*. Let* A *be the Néron model of* A_K*, and let* $G_K \to A_K$ *be a morphism of commutative group schemes over* K*. Then, the following hold.*

(1) *If one of the conditions* (i) *or* (ii) *holds, there exists a morphism* $G \to A$ *of commutative group schemes over* $\mathcal{O}$ *that extends* $G_K \to A_K$*.*
   (i) G *is étale over* $\mathcal{O}_K$*.*
   (ii) *If* p *is the characteristic of the residue field* F *of* K*, then the valuation* $e = \operatorname{ord}_K p$ *of* p *in* K *is less than* $p-1$*. Moreover, the connected component* $A_F = A \otimes_{\mathcal{O}} F$ *is an extension of an abelian variety by a torus.*

(2) *Suppose that* $G_K \to A_K$ *is a closed immersion and that either condition* (ii) *in* (1) *holds or* $e = p-1$ *and the degree of* G *is relatively prime to* p*. Then, the morphism* $G \to A$ *of commutative group schemes over* K *extending* $G_K \to A_K$ *is also a closed immersion.*

The case (i) in (1) is clear from the definition of Néron models. We omit the proof of the other cases.

COROLLARY D.13. *Let* A_K *be an abelian variety over* K*, and let* A *be its Néron model. Let* $I \subset G_K$ *be the inertia group.*

(1) *Let* N *be an positive integer relatively prime to* p*. Then, there is a natural isomorphism of the finite abelian group* $A_F[N](\overline{F}) \to A_K[N](\overline{K})^I$*.*

(2) *Let* ℓ *be a prime number different from the characteristic of the residue field. Then, there is a natural isomorphism of the finite-dimensional* $\mathbf{Q}_\ell$*-vector space* $V_\ell A_F \to (V_\ell A_K)^I$ *compatible with the action of the natural morphism* $G_K \to G_K/I = G_F$*. Suppose* F *is a perfect field, and let* A_F^{a} *be the abelian part of* A_F*, and let*

A^{t}_F be the torus part of A_F. Then, we obtain an exact sequence $0 \to V_\ell A^{\mathrm{t}}_F \to V_\ell A_F \to V_\ell A^{\mathrm{a}}_F \to 0$.

(3) *Let L be a finite Galois extension of K, let $I_{L/K} \subset \mathrm{Gal}(L/K)$ be the inertia group, and let E be the residue field of L. Suppose F is a perfect field, and let A^{a}_E be the abelian part of the closed fiber A_E of the Néron model of A_L, and let A^{t}_E be the torus part. Then, the natural morphisms $V_\ell A^{\mathrm{a}}_F \to (V_\ell A^{\mathrm{a}}_E)^{I_{L/K}}$ and $V_\ell A^{\mathrm{t}}_F \to (V_\ell A^{\mathrm{t}}_E)^{I_{L/K}}$ are isomorphisms.*

PROOF. (1) Since the multiplication-by-N morphism $[N] : A \to A$ is étale, $A[N]$ is étale over $\mathcal{O}_K$. Therefore, if $K^{\mathrm{ur}} = \overline{K}^I$ is the maximal unramified extension of K, the natural morphism $A[N](\mathcal{O}_K^{\mathrm{ur}}) \to A_F[N](\overline{F})$ is an isomorphism. By the definition of Néron model, $A[N](\mathcal{O}_K^{\mathrm{nr}}) \to A_K[N](K^{\mathrm{nr}}) = A_K[N](\bar{K})^I$ is also an isomorphism.

(2) By (1), $V_\ell A_F \to (V_\ell A_K)^I$ is an isomorphism. By Corollary A.50, we obtain the exact sequence $0 \to V_\ell A^{\mathrm{t}}_F \to V_\ell A_F \to V_\ell A^{\mathrm{a}}_F \to 0$.

(3) By (2), the natural morphism $A_F \otimes_F E \to A_E$ induces the isomorphism $V_\ell A_F \to (V_\ell A_E)^{I_{L/K}}$. By taking the $I_{L/K}$-invariant part of the exact sequence $0 \to V_\ell A^{\mathrm{t}}_E \to V_\ell A_E \to V_\ell A^{\mathrm{a}}_E \to 0$, we obtain $0 \to V_\ell A^{\mathrm{t}}_F \to V_\ell A_F \to V_\ell A^{\mathrm{a}}_F \to 0$ by Corollary A.50(2). ☐

COROLLARY D.14. *Let K be a discrete valuation field, and suppose its residue field F is perfect. Let ℓ be a prime number different from the characteristic of F.*

(1) *Let $A_K \to B_K$ be a morphism of abelian varieties over K, and let $A \to B$ be the morphism induced on their Néron models. Let $A^{\mathrm{t}}_F \subset A^0_F$ and $B^{\mathrm{t}}_F \subset B^0_F$ be the torus parts of the closed fibers. Suppose the kernel of $A_K \to B_K$ is finite. Then, $V_\ell A_K \to V_\ell B_K$ is injective. If we identify $V_\ell A_K$ and $V_\ell B_F$ as the subspaces of $V_\ell B_K$, we have $V_\ell A_F = V_\ell A_K \cap V_\ell B_F$ and $V_\ell A^{\mathrm{t}}_F = V_\ell A_K \cap V_\ell B^{\mathrm{t}}_F$.*

(2) *Let $X_K \to Y_K$ be a Galois covering of proper smooth curves over K, and let G be its Galois group. Let A_K and B_K be the Jacobians of X_K and Y_K, respectively. Let A_F and B_F be the closed fibers of the Néron models of A_K and B_K, and let A^{a}_F, B^{a}_F, A^{t}_F, B^{t}_F be their abelian parts and torus parts. We denote by ^{G} the G-invariant part. Then, the natural mappings $V_\ell A^{\mathrm{a}}_F \to (V_\ell B^{\mathrm{a}}_F)^G$ and $V_\ell A^{\mathrm{t}}_F \to (V_\ell B^{\mathrm{t}}_F)^G$ are isomorphisms.*

PROOF. (1) It is clear that $V_\ell A_K \to V_\ell B_K$ is injective. By Corollary D.13(2), $V_\ell A_F$ and $V_\ell B_F$ are invariant subspaces by the inertia group I. Thus, $V_\ell A_F = V_\ell A_K \cap V_\ell B_F$ follows from $(V_\ell A_K)^I = V_\ell A_K \cap (V_\ell B_K)^I$. By Corollary A.50(2), $V_\ell A_F^{\mathrm{a}} = V_\ell A_F / V_\ell A_F^{\mathrm{t}} \to V_\ell B_F^{\mathrm{a}} = V_\ell B_F / V_\ell B_F^{\mathrm{t}}$ is injective. Thus, $V_\ell A_F^{\mathrm{t}} = V_\ell A_K \cap V_\ell B_F^{\mathrm{t}}$.

(2) By Lemma D.6(2), $V_\ell A_K$ is identified with $(V_\ell B_K)^G$. Thus, by (1), we have $V_\ell A_F = (V_\ell B_F)^G$ and $V_\ell A_F^{\mathrm{t}} = (V_\ell B_F^{\mathrm{t}})^G$. Moreover, taking the G-invariant part of the exact sequence $0 \to V_\ell B_F^{\mathrm{t}} \to V_\ell B_F \to V_\ell B_F^{\mathrm{a}} \to 0$, we obtain the isomorphism $V_\ell A_F^{\mathrm{a}} \to (V_\ell B_F^{\mathrm{a}})^G$. ☐

Whether an abelian variety A_K over a discrete valuation field K has good reduction or semistable reduction can be determined by the ℓ-adic representation $V_\ell A$ of G_K.

DEFINITION D.15. Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let p be the characteristic of F. Let ℓ be a prime number that is invertible in K, and let V be an ℓ-adic representation of the absolute Galois group G_K.

(1) A projective system $G = (G_n)_{n \in \mathbf{N}}$ of surjections of finite flat commutative group schemes over $\mathcal{O}$ is called *ℓ-divisible group* if the following conditions are satisfied: $\ell^n : G_n \to G_n$ is the 0 morphism. $[\ell] : G_n \to G_n$ is decomposed into the surjection $G_n \to G_{n-1}$ and the closed immersion $i_{n-1} : G_{n-1} \to G_n$. The kernel of $[\ell] : G_n \to G_n$ is $i_{n-1} \circ \cdots \circ i_1 : G_1 \to G_n$.

(2) V is said to be a *good* ℓ-adic representation if there is an ℓ-divisible group such that $V = \varprojlim_n G_n(\overline{K}) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$.

(3) V is said to be a *semistable* ℓ-adic representation if there exist a good ℓ-adic representation $V_0 \subset V$ such that V/V_0 is unramified.

If $\ell \neq p$, then V is good if V is unramified. If $\ell = p$, the definition of good or semistable ℓ-adic representation is limited to this book, and they are much stronger conditions than usual ones.

LEMMA D.16. *Let p and ℓ be prime numbers, and let K be a finite extension of $\mathbf{Q}_\ell$. Let ρ be an ℓ-adic representation of $G_{\mathbf{Q}_p}$ to a two-dimensional K-vector space V. If the action of $G_{\mathbf{Q}_p}$ on* $\det V$ *is the ℓ-adic cyclotomic character, the following are equivalent.*

(1) *V is semistable in the sense of Definition* D.15.

(2) *V is semistable in the sense of Definition* 3.35.

PROOF. (2) ⇒ (1) is clear. We show (1) ⇒ (2). It suffices to show it assuming V has a good one-dimensional subrepresentation V_0 such that V/V_0 is unramified. By the assumption that the determinant

$\det V$ is the ℓ-adic cyclotomic character, the action of the inertia group I_p on V_0 is also the ℓ-adic cyclotomic character, and thus V is ordinary. ☐

The following is a generalization of Proposition 3.46.

THEOREM D.17. *Let K be a local field, and let A_K be an abelian variety over K. Let ℓ be a prime number different from the characteristic of K. In each of* (1) and (2), the conditions (i) and (ii) are equivalent.

(1) (i) A_K has good reduction.
(ii) The ℓ-adic representation V_ℓ of G_K is good.

(2) (i) A_K has semistable reduction.
(ii) The ℓ-adic representation V_ℓ of G_K is semistable.

(i) $\Rightarrow$ (ii) in (1) is clear from Lemma D.11. We omit the proof of the others.

D.4. The Néron model of the Jacobian of a curve

Let $\mathcal{O}$ be a discrete valuation ring, let X_K be a curve over its field of fractions. By Theorem D.3, if X_K has good reduction, so does its Jacobian $J_K = \operatorname{Pic}^0 X_K$. More precisely, we have the following.

LEMMA D.18. *Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field. Let X be a proper smooth curve over $\mathcal{O}$ such that each geometric fiber is connected. Then, the functor* $\operatorname{Pic}^0_{X/\mathcal{O}}$ *is represented by an abelian scheme J over $\mathcal{O}$. $J_K = J \otimes_{\mathcal{O}} K$ is the Jacobian of $X_K \otimes_{\mathcal{O}} K$, and J is the Néron model of J_K. The closed fiber $J_F = J \otimes_{\mathcal{O}} F$ is the Jacobian of $X_F = X \otimes_{\mathcal{O}} F$.*

For a prime number ℓ different from the characteristic of K, the ℓ-adic representation $V_\ell J_K$ of $\mathrm{Gal}(\overline{K}/K)$ *is a good ℓ-adic representation. If ℓ is different from the characteristic of F, the natural mapping $V_\ell J_K \to V_\ell J_F$ is an isomorphism of finite-dimensional* $\mathbf{Q}_\ell$*-vector spaces that is compatible with* $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(\overline{F}/F)$.

PROOF. It follows easily from Theorem D.3 and Lemma D.11. ☐

Even if a curve does not have good reduction, we have the following theorem on regular model.

THEOREM D.19. *Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field. Let X be a proper regular connected curve over $\mathcal{O}$ such that each geometric fiber is connected.*

Suppose $X_K = X \otimes_{\mathcal{O}} K$ is smooth, F is perfect, and the greatest common divisor of the multiplicities of components of $X_F = X \otimes_{\mathcal{O}} K$ in X_F is 1*. Then,*

1. *The functor $\operatorname{Pic}^0_{X/\mathcal{O}}$ is represented by the connected component J^0 of the Néron model J of the Jacobian J_K of X_K.*
2. *Let Γ be the dual chain complex of X_F, and let $\alpha_0 : \Gamma_0 \to \Gamma_0^*$ and $\beta : \Gamma_0^* \to \mathbf{Z}$ be the linear mappings in* (B.4) *and* (B.5)*, respectively. Then the group of connected components of the closed fiber $J_F = J \otimes F$ of the Néron model J is naturally isomorphic to* $\operatorname{Ker}\beta / \operatorname{Im}\alpha_0$.

Corollary D.20. *Let the notation be as is in Theorem* D.19. *Let $\overline{J}_F$ be the Jacobian of the normalization $\overline{X}_F$ of the reduced part of X_F. Then, the morphism $J_F \to \overline{J}_F$ induced by the natural morphism $\overline{X}_F \to X_F$ gives an isomorphism from the abelian variety part of the connected component J_F^0*

$$J_F^{\mathrm{a}} \to \overline{J}_F. \tag{D.18}$$

Proof. It is clear from Theorem D.19(1) and Theorem D.7(4). □

If a curve over a discrete valuation field has semistable reduction, so does its Jacobian. More precisely, we have the following.

Corollary D.21. *Let $\mathcal{O}$ be a discrete valuation ring, let K be its field of fractions, and let F be its residue field. Let X be a proper weakly semistable curve over $\mathcal{O}$ such that each geometric fiber is connected. Let J be the Néron model of the Jacobian J_K of $X_K = X \otimes_{\mathcal{O}} K$.*

1. *Let $\overline{X}_F$ be the normalization of X_F, and let $\Gamma = [\Gamma_1 \to \Gamma_2]$ be the dual chain complex of the closed fiber X_F. The connected component J_F^0 of the closed fiber $J_F = J \otimes_{\mathcal{O}} F$ is an extension of the Jacobian of $\overline{X}_F$ by a torus* $\operatorname{Hom}(H_1(\Gamma), \mathbf{G}_m)$.

   Let $C_1, \ldots, C_m$ be the components of $\overline{X}_F$, let Σ be the reduced closed subscheme of X_F consisting of singular points. Let g be the genus of X_F, F_i the field of definition of C_i, and let g_i be the genus of the curve C_i over F_i. Then we have

$$g = 1 + \deg\Sigma + \sum_{i=1}^{m} [F_i : F](g_i - 1). \tag{D.19}$$

(2) *The group of connected components of* J_F *is naturally isomorphic to the cokernel of the linear mapping* $\bar{\alpha}_1 : H_1(\Gamma) \to H^1(\Gamma^\vee)$ *of* (B.8).

PROOF. (1) Let X' be the minimal resolution of singularities of X. We have $X_K = X'_K$. Since all the exceptional divisors are of genus 0, the Jacobian of the normalization of X'_F equals that of $\overline{X}_F$. If Γ' is the dual chain complex of X'_F, then by Proposition B.14(1), we have a natural isomorphism $H_1(\Gamma) \to H_1(\Gamma')$. Thus, by replacing X by X', we may assume X is semistable. By Theorem D.19(1) and Theorem D.7(3), J^0_F is an extension of the Jacobian by a torus. Then, by Corollary D.21, the character group of the torus part of J^0_F equals $H_1(\Gamma)$.

Let a be the dimension of the abelian variety part of J_F, and let t be that of the torus part. Then, we have $g = a + t$. Since $a = \sum_{i=1}^m [F_i : F] g_i$ and $t - 1 = \deg \Sigma - \sum_{i=1}^m [F_i : F]$, we have (D.19).

(2) As in (1), we may replace X by X' by Proposition B.14(1). The assertion follows from Theorem D.19(2) and Proposition B.14(2). □

COROLLARY D.22. *Let* K *be a discrete valuation field, let* X_K *be a proper smooth curve over* K*, and let* J_K *be the Jacobian* X_K*. If* X_K *has semistable reduction, so does the Jacobian* J_K*.*

For a prime number ℓ *different from the characteristic of* K*, the* ℓ*-adic representation* $V_\ell J_K$ *of* $\mathrm{Gal}(\overline{K}/K)$ *is a semistable* ℓ*-adic representation.*

PROOF. It follows from Corollary D.21(1) and Theorem D.17(2) (i) ⇒ (ii). □

Bibliography

References for theorems and propositions that were not proved in the text

CHAPTER 8

[1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., Springer, **106**, 1986.

[2] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques,* in Modular Functions of One Variable II, Lecture Notes in Math., Springer, **349**, 1973, 143–316.

[3] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Annals of Math. Studies, Princeton Univ. Press, **151**, 1994.

[4] H. Hida, *Geometric modular forms and elliptic curves*, World Scientific, 2000.

[5] B. J. Birch, W. Kuyk (eds.), *Modular Functions of One Variable IV*, Lecture Notes in Math., Springer, **476**, 1973.

- ◇ Lemma 8.37: [**2**] III Corollaire 2.9, p.211, [**3**] Corollary 4.7.2.
- ◇ Lemma 8.41: $p = 2, 3$: [**1**] Appendix A, Proposition 1.2 (c).
- ◇ Example 8.65: [**5**] Table 6, p.143.
- ◇ Proposition 8.69: [**2**] VII Costruction 1.15, p.297.
- ◇ Theorem 8.77: [**2**] V Théorème 2.12, [**3**] Theorem 13.11.4.

CHAPTER 9

[6] H. Carayol, *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke Math. J. 59 (1989), 785–801.

[7] T. Miyake, *Modular forms.* Translated from the Japanese by Yoshitaka Maeda. Springer-Verlag, Berlin, 1989. x+335 pp.

[8] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Inventiones Math., **100** (1990), 431–476.

◇ Theorem 3.55(2) (ii) ⇒ (i): [**6**].
◇ Theorem 9.40: [**7**] Corollary 4.6.20.
◇ Theorem 3.55(1) (ii) ⇒ (i) the case $p \equiv 1 \bmod \ell$: [**8**].

CHAPTER 10

[9] J.-P. Serre, *Arbres, amalgames*, SL_2, Astérisque 46, Société Mathématique de France, Paris, 1977.
[10] ———, *Le problème des groupes de congruence pour* SL_2, Ann. of Math. 92 (1970), 489–527.
[11] L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig, 1901.

◇ Theorem 10.15(1): [**9**] Chapitre II 1.4 Théorème 3 p.110.
◇ Theorem 10.15(2): [**10**] 2.6 Corollaire 3 p.449 (If we let $K = \mathbf{Q}$, $S = \{p, \infty\}$, and $\mathfrak{q} = (N)$, then we have $\Gamma_{\mathfrak{q}} = \tilde{\Gamma}(N)$ and $E_{\mathfrak{q}} = \tilde{E}(N)$.)
◇ Theorem 10.28: [**11**] sections 255, 260.

CHAPTER 11

[12] J.-P. Serre, *Corps Locaux*, 3e ed., Hermann, Paris, 1980.
[13] ———, *Cohomologie galoisienne*, 5e ed., Lecture Notes in Math., Springer-Verlag, Berlin, **5**, 1994.
[14] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Math. 1, Academic Press, Boston, 1986.

◇ General theory of Galois cohomology and duality theorem: [**4**].
◇ Proposition 11.11(1): [**12**] Chapitre X §3 b), (2): ibid., Proposition 9.
◇ Proposition 11.18: [**14**] Corollary 2.3.
◇ Proposition 11.20: [**14**] Theorem 2.8.
◇ Proposition 11.25(1): [**14**] Corollary 4.15.
◇ Proposition 11.25(2): [**14**] Theorem 4.10.
◇ Proposition 11.27: [**14**] Theorem 5.1.

APPENDIX B

[65] P. Deligne, N. Katz, *Groupes de Monodromie en Géométrie Algébrique* (SGA 7) II, Lecture Notes in Math., Springer, **340**, (1973).

Lemma B.4 (iii) ⇒ (i) The case where k is general: [**65**] Exp. XV, Théorème 1.2.6.
Lemma B.12: [**65**] Exp. X, Corollaire 1.8.

APPENDIX C

[15] J.-M. Fontaine, *Groupes p-divisible sur les corps locaux*, Astérisque 47–48, Soc. Math. de France, 1977.
[16] J.-M. Fontaine, G. Laffaille, *Construction de représentations p-adiques*, Ann. Sci. École Norm. Sup. (4) 15 (1982), 547–608 (1983).
[17] N. Wach, *Représentations cristallines de torsion*, Compositio Math. 108 (1997), 185–240.

◇ Theorem C.1:[**15**] Chapitre III.
◇ Theorem C.6:[**16**], [**17**].

APPENDIX D

[18] S. Mukai, *An introduction to invariants and moduli*, Translated from the 1998 and 2000 Japanese editions by W. M. Oxbury. Cambridge Studies in Advanced Mathematics, 81. Cambridge University Press, Cambridge, 2003. xx+503 pp.
[19] M. Artin, *Néron models*, in G. Cornell, J. Silverman, (eds.), Arithmetic Geometry, Springer, 1986 pp.213–230.
[20] J. S. Milne, *Jacobian varieties,* in G. Cornell, J. Silverman, (eds.), Arithmetic Geometry, Springer, 1986 pp.167–212.
[21] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Springer, 1990.
[22] M. Raynaud, *Jacobienne des courbes modulaires et opérateurs de Hecke,* in “Courbes modulaires et courbes de Shimura”, Astérisque 196–197, Soc. Math. de France, 1991, 9–25.

[23] A. Grothendieck, *Modèles de Néron et monodromie*, in Groupes de Monodromie en Géométrie Algèbrique, SGA 7I, Lecture Notes in Math., Springer, **288**, 1972, 313–523. Proposition 5.13.

◇ Jacobians and Néron models: [**19**], [**20**], [**21**]

◇ Curves and their Jacobians: [**18**] Chapter 8.

◇ Abel's theorem: [**18**] Theorem 9.8.6.

◇ Theorem D.3: [**21**] Theorems 8.4/3 and 9.3/1.

◇ Theorem D.7: [**21**] Theorem 8.2/3 and Propositions 9.2/5 and 10.

◇ Theorem D.8: [**21**] Corollary 1.3/1.

◇ Proposition D.12: [**22**], Proposition 6.

◇ Theorem D.17(1) $\ell \neq p$: [**21**] Theorem 7.4/5 (b)$\Leftrightarrow$(d).

◇ Theorem D.17(2) $\ell \neq p$: [**21**] Theorem 7.4/6.

◇ Theorem D.17(2) $\ell = p$: [**23**] Proposition 5.13.

◇ Theorem D.19(1): [**21**] Theorem 9.5/4, p.267.

◇ Theorem D.19(2): [**21**] Theorem 9.6/1, p.274.

Symbol Index

$\cup$, 149
1-cocycle, 144

α_q, 125
$\langle a \rangle$, 22
$\langle a \rangle^{-1/2}$, 132
A_f, 111, 131
$A_{\Sigma'}$, 113

$\mathrm{Br}(F)$, 150
${}_nBr(F)$, 150

$C^q(G, M)$, 149
$C(X, \mathcal{F})$, 137

Δ_Q, 126
Δ_q, 125
Δ_p, 117
$\mathrm{Def}_{R\text{-}G}(M)$, 146
$\mathrm{Def}^0_{R\text{-}G}$, 146
$\mathrm{Def}_{\bar{\rho}, \mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{[V_n]}$, 163
$\mathrm{div}\, f$, 199
$D(G)$, 191, 194
$D(\bar{\rho})$, 108
$D(X)$, 199

ε, 70
ε_f, 70
$\bar{e}$, 51
e_x, 24
$E(N)$, 118
$\tilde{E}(N)$, 118
$E^{(p^e)}$, 2
$E_{q_r^r}$, 51
$\mathrm{End}^0_R(M)$, 147
$\mathrm{Ext}_{R\text{-}G}(M, N)$, 148

f_a, 65
$f_Q^\natural$, 132
F, 2, 191, 193
F_e, 2
F_S, 1
$\mathcal{F}_{\Sigma', \Sigma}$, 116

$\Gamma_{0,*}(p, N)$, 118
$\Gamma(N)$, 118
$\Gamma_1(N)$, 38
$\tilde{\Gamma}(N)$, 118
$\Gamma(r)$, 29
G-coinvariant, 144
$G^\times$, 10
$G_{(a,b)}$, 33
G_F, 143
G_S, 155
$\mathrm{Grass}(\mathcal{O}_{E[N]}, N)$, 41

$H^0(G, M)$, 144
$H^1(G, M)$, 144
$H^1_f(\mathbf{Q}_\ell, W_n)$, 161
$H^1_f(\mathbf{Q}_p, M)$, 151
$H^1_f(\mathbf{Q}_p, \mathrm{Hom}_R(M, N))$, 152

$H^1_f(\mathbf{Q}_p, N)$, 152
$H^1_s(\mathbf{Q}_\ell, W_n)$, 162
$H^q(F, M)$, 150
$H^q(G, M)$, 149

i_Σ, 110
$I_0(N, n)$, 62
$I_1(N, n)$, 66
$\mathcal{I}_0(N, n)$, 62
$\mathrm{Ig}(Mp^a, r)_{\mathbf{F}_p}$, 33
$\mathrm{Ig}(Mp^a, r)^{P=0}_{\mathbf{F}_p}$, 34
$\overline{\mathrm{Ig}}(Mp^a, r)_{\mathbf{F}_p}$, 56

j, 21, 29
j_a, 35, 42, 55, 56
j_0, j_1, 49, 58, 59, 118
$J_{0,1}(N, M)$, 70
$J_0(N)_{\mathbf{Q}}$, 61
$J_1(N)_{\mathbf{Q}}$, 66

K_f, 63

λ, 31
ℓ-divisible group, 208
$(L_p)_{p \in S}$, 157
$(L_p^\vee)_{p \in S}$, 158
L_Σ, 162
$\mathrm{Lift}^0_{R\text{-}G}$, 146
$\mathrm{Lift}_{R\text{-}G}(M)$, 146
$\mathrm{Lift}_{\bar\rho, \mathcal{D}_\Sigma}(\mathcal{O}/(\pi^n)[\varepsilon])_{V_n}$, 163

μ, 25
$\mu_N^\times$, 12
$m^\natural_Q$, 130
$m^\natural_{\varnothing,Q}$, 135
$m^*_{\Sigma',\Sigma}$, 114
$m_{\Sigma',\Sigma}$, 115
$\mathfrak{m}'_Q$, 131
$\mathfrak{m}_{R_\Sigma}$, 163
$\mathfrak{m}_\Sigma$, 110
$\mathfrak{m}'_\Sigma$, 110

$\tilde{M}$, 146
$\widetilde{M}_{\tilde\rho}$, 146
$M_0(N)_E$, 41
$M_1(N)_E$, 15
$M(1)$, 150
M^G, 144
M_G, 144
$M^\natural_Q$, 134
M_Σ, 114
$M^\vee$, 150
$\mathcal{M}$, 21
$\mathcal{M}_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$, 25
$\mathcal{M}_0(N)$, 20
$\mathcal{M}_0(N)_E$, 13
$\mathcal{M}_0(N)_{\mathbf{F}_p}$, 23
$\mathcal{M}_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$, 25
$\mathcal{M}_{1,0}(M, N)$, 57
$\mathcal{M}_1(N)$, 20
$\mathcal{M}_1(N)_E$, 13
$\mathcal{M}(r)_{\mathbf{Z}[\frac{1}{r}]}$, 25

$N_f\mathcal{L}$, 202
N-Isog_E, 41

ord, 2

$\overline{\varphi}_\Sigma$, 108
$\mathbf{\Phi}$, 97
p_{R_Σ}, 163
$\langle P \rangle$, 13
$P_{f,p}(U)$, 111, 131
$P_p(U)$, 94, 109
$P_q(U)$, 130
$P_{X/S}(T)$, 202
$\mathrm{Pic}(X)$, 199, 201
$\mathrm{Pic}^0(X)$, 202
$\mathrm{Pic}^0_{X/S}$, 203
$\mathrm{Pic}_{X/k}$, 202

Q, 126
$\mathcal{Q}$, 126
$\widetilde{\mathcal{Q}}$, 125
$\mathbf{Q}_S$, 155

$\mathcal{R}^{\natural}_{Q}$, 135
$\mathcal{R}_{\Sigma}$, 114
$R[\varepsilon]$, 146

s_0, s_1, 118
s_d, 45, 59
s_k, 82
$s_k(q)$, 50
$S_0(N)$, 61
$S_1(N)$, 66
S^{ss}, 2
$\mathrm{Sel}(E, n)$, 158
$\mathrm{Sel}_L(M)$, 157
$\mathrm{Sel}_{\Sigma}(W_n)$, 162

t_k, 82
$\tilde{t}_{\varnothing,Q}$, 129
$t^{\flat}_{\Sigma',\Sigma}$, 113
$t^{\natural}_{\varnothing,Q}$, 130
$T(N)_{\mathbf{Z}}$, 108
$T(N_{\Sigma})'_{\mathcal{O}}$, 110
$T[N]$, 16
$T^{(N)}$, 16
$T_{\ell}J_0(N)$, 70
$T_0(N)_{\mathbf{Z}}$, 62
$T_1(N)_{\mathbf{Z}}$, 67
$T_{N,E}$, 41
$T^{\flat}_{\Sigma}$, 110
$T^{\natural}_{Q}$, 130
$T^{\sharp}_{\ell}$, 113
$T^{\sharp}_{q}$, 129
$\boldsymbol{T}$, 97
$\boldsymbol{T}'$, 103
Tor, 137

U_{ℓ}, 115
U_p, 92, 115

V, 2, 72, 161, 191
V^0_n, 161
V_e, 2
V_f, 71
$V_{\ell}J_0(N)$, 70

$w^2_{N'}$, 22
W, 161
W^0_n, 162

$X_0(N)_{\mathbf{Z}}$, 48
$X_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$, 54
$X_1(Mp)^{\mathrm{bal}}_{\mathbf{Z}[\zeta_p]}$, 59
$X_1(N)_{\mathbf{Z}}$, 48
$X_{1,*}(Mp, r)^{\mathrm{bal}}_{\mathbf{Z}[\frac{1}{r},\zeta_p]}$, 58
$X_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$, 54
$X_{1,0}(M, N)_{\mathbf{Z}}$, 58
$X_{1,0}(N, M)_{\mathbf{Z}}$, 58
$X^{(p)}$, 1
$X(1)_{\mathbf{Z}}\ |^{\wedge}_{\infty}$, 51

$Y_{0,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$, 42
$Y_0(N)_{\mathbf{Z}}$, 23
$Y_1(4)$, 20, 47
$Y_{1,*}(N, r)_{\mathbf{Z}[\frac{1}{r}]}$, 31
$Y_{1,0}(M, N)_{\mathbf{Z}}$, 57
$Y_1(N)^{\mathrm{an}}$, 38
$Y_1(N)_{\mathbf{Z}}$, 24
$Y(1)_{\mathbf{Z}}$, 29
$Y(2)$, 31
$Y(3)$, 25
$Y(r)^{\mathrm{an}}$, 29
$Y(r)_{\mathbf{Z}[\frac{1}{r}]}$, 26

$Z^1(G, M)$, 144
$\widehat{\mathbf{Z}}$, 144
$\mathbf{Z}((q))$, 51

Subject Index

absolute Frobenius morphism, 1
annihilator, 153
Atkin–Lehner involution, 23

Brauer group, 150

character
  of f, 70
congruence relation, 73
connected component, 205
cup product, 149
curve, 179
cyclic group scheme, 9

diamond operator, 22, 67
Dieudonné module, 191
divisor, 199
divisor class group, 199
divisor group, 199
Drinfeld level structure, 13
dual chain complex, 182
dual local condition, 158

Eisenstein ideal, 77
étale
  filtered φ-module, 192
exact order N, 13
extension, 147, 196

filtered φ-module, 192
finite G-module, 143
finite R-G-module, 143
Frobenius morphism, 23
full Hecke algebra, 110, 130
full set of sections, 6

G-coinvariant, 144
generator, 9
genus, 179
good, 208
good reduction, 182, 205

Hecke algebra, 62, 67
Hecke module, 114, 134
Hecke operator, 67

Igusa curve, 33
index, 182
infinitesimal deformation, 146
infinitesimal lifting, 146

Jacobian, 203

ℓ-divisible group, 208
local condition, 157

minimal resolution of singularities, 188
multiplicative
  filtered φ-module, 192

Néron model, 205
node, 180
non-Eisenstein, 123
non-Eisenstein ideal, 78
norm
  of an invertible sheaf, 202

old part, 91
1-cocycle, 144
ordinary, 2

perfect complex, 136
Petersson product, 65, 68
Picard functor, 202
Picard group, 201
preserve the determinant, 146
primary form, 70
principal divisor, 199
profinite group, 143

relative Frobenius morphism, 2
right bounded, 136

scheme of generators, 10
Selmer group, 157
  of an elliptic curve, 158
semistable, 182, 208
semistable reduction, 182, 205
singular chain complex, 137
strongly divisible, 192
supersingular, 2

Tate curve, 51
Tate twist, 150

unramified part, 151

weakly semistable, 182

Selected Published Titles in This Series

245 **Takeshi Saito,** Fermat's Last Theorem, 2014

243 **Takeshi Saito,** Fermat's Last Theorem, 2013

242 **Nobushige Kurokawa, Masato Kurihara, and Takeshi Saito,** Number Theory 3, 2012

240 **Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito,** Number Theory 2, 2011

235 **Mikio Furuta,** Index Theorem. 1, 2007

230 **Akira Kono and Dai Tamaki,** Generalized Cohomology, 2006

227 **Takahiro Kawai and Yoshitsugu Takei,** Algebraic Analysis of Singular Perturbation Theory, 2005

224 **Ichiro Shigekawa,** Stochastic Analysis, 2004

218 **Kenji Ueno,** Algebraic Geometry 3, 2003

217 **Masaki Kashiwara,** *D*-modules and Microlocal Calculus, 2003

211 **Takeo Ohsawa,** Analysis of Several Complex Variables, 2002

210 **Toshitake Kohno,** Conformal Field Theory and Topology, 2002

209 **Yasumasa Nishiura,** Far-from-Equilibrium Dynamics, 2002

208 **Yukio Matsumoto,** An Introduction to Morse Theory, 2002

207 **Ken'ichi Ohshika,** Discrete Groups, 2002

206 **Yuji Shimizu and Kenji Ueno,** Advances in Moduli Theory, 2002

205 **Seiki Nishikawa,** Variational Problems in Geometry, 2002

201 **Shigeyuki Morita,** Geometry of Differential Forms, 2001

199 **Shigeyuki Morita,** Geometry of Characteristic Classes, 2001

197 **Kenji Ueno,** Algebraic Geometry 2, 2001

195 **Minoru Wakimoto,** Infinite-Dimensional Lie Algebras, 2001

189 **Mitsuru Ikawa,** Hyperbolic Partial Differential Equations and Wave Phenomena, 2000

186 **Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito,** Number Theory 1, 2000

185 **Kenji Ueno,** Algebraic Geometry 1, 1999

183 **Hajime Sato,** Algebraic Topology: An Intuitive Approach, 1999

For a complete list of titles in this series, visit the
AMS Bookstore at **www.ams.org/bookstore/mmonoseries/**.

This is the second volume of the book on the proof of Fermat's Last Theorem by Wiles and Taylor (the first volume is published in the same series; see MMONO/243). Here the detail of the proof announced in the first volume is fully exposed. The book also includes basic materials and constructions in number theory and arithmetic geometry that are used in the proof.

In the first volume the modularity lifting theorem on Galois representations has been reduced to properties of the deformation rings and the Hecke modules. The Hecke modules and the Selmer groups used to study deformation rings are constructed, and the required properties are established to complete the proof.

The reader can learn basics on the integral models of modular curves and their reductions modulo p that lay the foundation of the construction of the Galois representations associated with modular forms. More background materials, including Galois cohomology, curves over integer rings, the Néron models of their Jacobians, etc., are also explained in the text and in the appendices.

For additional information
and updates on this book, visit

www.ams.org/bookpages/mmono-245

ISBN 978-0-8218-9849-9

9 780821 898499

MMONO/245

AMS *on the* Web
www.ams.org